DISEÑO ADMINISTRATIVO PARA LA CREACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA CSIRT EN LA EMPRESA PLATINO SISTEMAS.

WILLIAN ALEXANDER FRANCO REYES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA-BOYACA
2020

DISEÑO ADMINISTRATIVO PARA LA CREACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA CSIRT EN LA EMPRESA PLATINO SISTEMAS.

WILLIAN ALEXANDER FRANCO REYES

TRABAJO DE GRADO PROYECTO APLICADO

DIRECTOR: DANIEL FELIPE PALOMO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA-BOYACA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Tunja día _____, mes _____, año____

A mi esposa Jenny Chávez, que siempre me brinda todo su apoyo incondicional, así como el tiempo y los medios necesarios para plasmar todas mis ideas en el entorno académico y laboral. A mis hijas Sara Sofia y Ana Lucia Franco, quienes son mi inspiración y motivo para superarme profesionalmente.

AGRADECIMIENTOS

Agradezco a Dios todo poderoso por permitir encaminarme en un área de profundización tan interesante en mi profesión, por brindarme la claridad, inteligencia y sabiduría para el desarrollo de las temáticas propuesta por mi institución.

A mi alma mater y todo su cuerpo docente por brindarme los conocimientos, afianzar mis habilidades y por orientarme en el desarrollo de esta especialización en seguridad informática.

Agradezco a mi familia, esposa e hija, quienes me brindan el apoyo emocional y académico para desarrollar cada una de las actividades que me forman como profesional.

A todos los docentes que han formado parte de mi crecimiento personal, académico y profesional, desde mi escuela, colegio y universidad, porque me han brindado parte de sus conocimientos para amoldarlos a mis necesidades.

RESUMEN

Este proyecto tiene como finalidad diseñar un documento que permita el desarrollo y establecimiento de las actividades de un centro de respuesta a incidentes de seguridad informática CSIRT, en la empresa PLATINO SISTEMAS, una organización colombiana que presta servicios para asegurar y proteger la información.

El principal objetivo del proyecto es establecer la estructura organizacional del equipo de respuesta a incidentes informáticos, para la empresa PLATINO SISTEMAS, en donde se identifiquen claramente aspectos en su organización como perfiles de los profesionales a cargo de la respuesta a incidentes y atención de vulnerabilidades, así el ámbito de actuación y los tipos de servicios a ofrecer por parte de la organización.

Mediante el análisis del panorama en Colombia acerca del establecimiento de equipos de respuesta CSIRT, estudios de factibilidad, establecimiento del ámbito de actuación de estos equipos y la definición de las políticas y procedimientos a seguir por parte de los centros de respuesta, se realizará la redacción de un documento que defina la composición y actuación del equipo de respuesta CSIRT para la empresa PLATINO SISTEMAS, que será capaz de crear y gestionar las diferentes funciones de respuesta a incidentes cibernéticos.

Palabras Clave: Seguridad Informática, respuesta a incidentes, servicios reactivos, servicios proactivos, seguridad digital, gestión de riesgo, amenazas cibernéticas.

ABSTRACT

The purpose of this project is to design a document that allows the development and establishment of the activities of a CSIRT computer security incident response center, in the company PLATINO SISTEMAS, a Colombian organization that provides services to ensure and protect information.

The main objective of the project is to establish the organizational structure of the computer incident response team, for the company PLATINO SISTEMAS*, where aspects of its organization are clearly identified, such as profiles of professionals in charge of incident response and vulnerability attention, thus the scope of action and the types of services to be offered by the organization.*

By analyzing the panorama in Colombia about the establishment of CSIRT response teams, feasibility studies, establishing the scope of action of these teams and defining the policies and procedures to be followed by the response centers, the writing will be carried out of a document that defines the composition and performance of the CSIRT response team for the company PLATINO SISTEMAS, which will be able to create and manage the different functions for responding to cyber incidents.

Key Words*: Computer Security, incident response, reactive services, proactive services, digital security, risk management, cyber threats.*

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE GRÁFICAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

INTRODUCCIÓN

La Seguridad informática según la ISO 27001 está basada en la preservación de la confidencialidad, integridad y disponibilidad de los datos o información de una organización, estableciendo estas tres propiedades como los pilares de la seguridad informática, por lo cual, todo ambiente laboral, académico, investigativo, gubernamental o cualquier otro que haga uso de Tecnologías de Información para la gestión de datos de importancia, deberán implementar métodos y herramientas que sean capaces de ofrecer un servicio de respuesta ante riesgos e incidentes informáticos, los cuales buscaran mantener los pilares de la seguridad informática dentro de la organización.

Del concepto anteriormente descrito surge la necesidad de implementar un mecanismo de respuesta rápido, eficiente y con las herramientas necesarias para prestar atención y dar solución a diferentes incidentes en el área informática; tal es el caso de los CSIRT (*Computer Security Incident Response Team)*, por sus siglas en inglés o Centros de Respuesta a incidentes de Seguridad Informática) los cuales son equipos de respuesta conformados por profesionales informáticos, con los conocimientos y habilidades profesionales necesarias para desarrollar medidas preventivas y reactivas ante un incidente en sistemas de información.

De esta manera la empresa PLATINO SISTEMAS, organización colombiana que actúa en el ámbito de la prestación de servicios de protección informática, desea implementar para el año 2022 un equipo capaz de dar servicio y soporte a diferentes clientes en el área de seguridad informática, de acuerdo con un nivel de servicio contratado.

Por lo anterior, este proyecto se centrará en realizar la descripción de los conceptos fundamentales de un equipo de respuesta, en donde se definirá el ámbito de actuación del CSIRT, la taxonomía de los ataques relevantes en medio de la situación actual colombiana, así como la definición de los tipos de servicios a ofrecer por el equipo, tanto reactivos, proactivos y complementarios.

.

Al finalizar se hará la entrega de una estructura clara y definida de las políticas y procedimientos operacionales del CSIRT, basados en los controles propuestos en los anexos de la norma ISO 27001, así como los requisitos y perfil profesional del equipo de trabajo que conforme el centro de respuesta.

1. DEFINICION DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

PLATINO SISTEMAS, es una empresa colombiana que actualmente ofrece servicios de seguridad y protección a la información. Esta empresa tiene como misión crear un centro o equipo de respuesta, el cual sea capaz de ofrecer servicios de atención ante incidentes informáticos y evaluación de vulnerabilidades, el cual este enfocado a diferentes usuarios de acuerdo con la actividad económica, comercial o de servicios que estos presten.

En medio de esta misión, se plantea que los servicios a ofrecer por el equipo de respuesta sean acordes al nivel contratado por ellos, los cuales podrán ser de respuesta a incidentes o de gestión a vulnerabilidades.

Actualmente la empresa no cuenta con un diseño o marco documental que permita dar desarrollo a la implementación de un equipo de trabajo que sea capaz de atender a los requerimientos trazados por la compañía, los cuales sean capaces de gestionar de manera ordenada y estructurada diferentes tipos de ataques cibernéticos.

1.2 FORMULACION DEL PROBLEMA

Por lo anterior, y analizando el escenario de la organización, se formula la siguiente pregunta problemática, ¿Cuál debe ser el diseño documental que permita dar desarrollo a las actividades propias de un centro de respuesta a incidentes informáticos en la empresa PLATINO SISTEMAS?

2. JUSTIFICACIÓN

Gracias al auge tecnológico, al crecimiento exponencial de las redes informáticas y el uso, cada vez mayor, de plataformas tecnológicas para realizar labores cotidianas, la comunidad tecnológica se ve expuesta a diferentes ataques cibernéticos, los cuales tiene diferentes objetivos, como el robo de información, suplantación de identidad o en algunos casos más simples el monitoreo de actividades e información personal, con el fin de ser vendidas a empresas que desean ofrecer productos y servicios a diferentes tipos de usuario.

Por lo cual surge la necesidad de la creación de medidas que permitan ofrecer ayuda a diferentes usuarios que se han visto afectados a través del espacio cibernético. Algunas de estas medidas son de carácter local, es decir, cada usuario cuenta con algunas medidas preventivas, para evitar ser infectados por virus informáticos; como antivirus, *antispyware* o *firewalls*, medidas que en su gran mayoría vienen instaladas y configuradas por defecto en los sistemas operativos de sus equipos de cómputo personal.

De igual manera existen otros tipos de riesgos o amenazas que son más complejas, por ende, la detección y prevención de estas deberá ser tratada de otra manera. Ejemplos de este tipo de amenazas son la ingeniería social, casos de suplantación de identidad, *phishing*, *ransomware* o amenazas persistentes avanzadas (APT), la cual combina diferentes métodos y técnicas de intrusión, para obtener la información de la víctima.

Con base a lo mencionado anteriormente se hace necesario que existan organizaciones que sean capaces de ofrecer asesoría, consultoría y ayuda a los usuarios del ciberespacio, grupos como los centros de Respuesta a Incidentes de Seguridad Informática, los cuales a través de diferentes servicios puedan brindar el apoyo suficiente a diferentes usuarios sin importar el ámbito en el que desarrollen sus actividades. La empresa PLATINO SISTEMAS es una de estas compañías, la cual basa su actividad organizacional en ofrecer este tipo de ayuda, por lo cual se hace necesario incluir dentro de su estructura orgánica, el diseño e implementación de un centro de respuesta CSIRT el cual sea capaz de brindar atención inmediata a los diversos ataques del ciberespacio. Por estas razones se encuentra muy importante la implementación de este proyecto, así como establecer el ámbito de actuación del CSIRT de la empresa, sus servicios y perfiles profesionales para la atención de incidentes de seguridad informática.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Definir la estructura organizacional y los tipos de servicios a ofrecer por parte de un Centro de Respuesta a Incidentes de Seguridad Informática CSIRT, para dar respuesta a incidentes cibernéticos en la empresa Platino Sistemas.

3.2 OBJETIVOS ESPECÍFICOS

Definir el ámbito de actuación y los servicios proactivos y reactivos que ofrecerá el CSIRT en la empresa PLATINO SISTEMAS a través del análisis del panorama actual de la ciberseguridad en Colombia.

Determinar los perfiles, requisitos y habilidades que debe tener el personal técnico y administrativo para la conformación del CSIRT y crear su estructura orgánica

Precisar las políticas y procedimientos operacionales con los cuales el CSIRT operará para dar respuesta a incidentes y evaluación de vulnerabilidades cibernéticos.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

Gracias al crecimiento exponencial de las redes tecnológicas y a las aplicaciones que soportan redes como internet, cada vez son mayores los registros o reportes realizados por usuarios de redes sociales, comerciantes de internet, agentes bancarios, entre otros acerca de los ataques informático que sufren en sus plataformas. En Colombia, recientemente se han revelado datos o noticias referentes a este tema tan delicado, en diarios como el tiempo se han publicado reportes, en los cuales se mencionan algunas tácticas y sectores que actualmente amenazan a los colombianos[1], refiriendo a las entidades bancarias como el blanco principal de los ciberdelincuentes. Por estas razones se hace necesario que se implementen medias que permitan brindar ayuda y atención a este tipo de incidentes, que, aunque sean informáticos, cada día cobran mayor importancia.

4.1.1 El contexto de un CSIRT. La organización de los estados americanos OEA define un CSIRT como “Un equipo de respuesta a incidentes en seguridad informática (CSIRT por sus siglas en inglés) es una organización cuyo propósito principal consiste en brindar servicios de respuesta a incidentes de seguridad informática a una comunidad en particular”.

Estos CSIRT, en muchas ocasiones, se encuentran constituidos como un grupo dentro de una organización que se encuentra dispuesta a ofrecer algún tipo de servicio en concreto. Estos servicios se encuentran englobados en áreas como la academia, entes gubernamentales o militares, comerciales, así como en pequeñas o medianas empresas que ofrecen diferentes servicios. Estos equipos de respuesta, han ido evolucionando con el paso del tiempo y de acuerdo a las necesidades de las organizaciones que los rodean, ya que en principio estos prestaban servicio y atención a niveles informáticos básicos, que no implicaban soluciones complejas, ahora, debido a la creciente ola de ataques y delitos informáticos, estos equipos ofrecen servicios de auditoria, análisis y gestión de riesgos en muchas áreas, inclusive en el combate diario contra *malware* y virus informáticos, tal como lo

[1] El tiempo. Las tácticas que amenazan su seguridad informática. [En línea]. [Consulta febrero 12 de 2020]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-ataques-de-cibercriminales-en-colombia-371096

menciona la OEA dentro de la definición mencionada para un CSIRT[2]. Hoy en día estos equipos se han conformado como centros de respuesta proactivos que se acoplan dentro de un sistema integral de gestión de seguridad que se centran en la prevención y detención de incidentes informáticos.

4.1.2 Ámbitos de actuación de un CSIRT. Como se mencionó anteriormente los equipos de respuesta a incidentes se desempeñan en diferentes áreas a lo cual se denomina ámbito de actuación del CSIRT, lo cual según la OEA pueden clasificarse de manera general en los siguientes grupos:

4.1.2.1 CSIRT Académicos. Equipos de respuesta enfocados a la atención de incidentes informáticos en comunidades académicas, como universidades, colegios, preparatorias, facultades o institutos educativos. El crecimiento y desarrollo de estos CSIRT dependen de la necesidad de la comunidad educativa a la que prestan sus servicios.

4.1.2.2 CSIRT Comerciales. A menudo las organizaciones empresariales externalizan este tipo de servicio, por lo cual, empresas ajenas al ente comercial ofrecen la posibilidad de a través de un medio de pago cubrir las necesidades de gestión y atención de incidentes informáticos.

4.1.2.3 CSIRT de Infraestructuras Criticas. Existen equipos de atención a respuesta en medio de ámbitos, donde específicamente se protegen la integridad de los activos de una organización, esto sin importar si la organización hace parte de sectores públicos o privados. Dada la importancia de este tipo de servicios y a que un gran número de comunidades de diferentes instituciones dependen de este CSIRT en concreto, se hace necesario establecer políticas de interacción entre los involucrados.

4.1.2.4 CSIRT Gubernamentales. Los equipos de respuesta gubernamentales se encargan de garantizar que todos los servicios de gobierno en Tecnologías y de la

[2] OEA. Buenas Prácticas para establecer un CSIRT nacional. [en línea]. [Consulta abril 14 de 2020]. Disponible en: https://www.sites.oas.org/cyber/Documents/2016 - Buenas Prácticas CSIRT.pdf

información, así como los servicios prestados a la ciudadanía cuenten con los niveles de seguridad adecuados y recomendados según sea el escenario o ambiente de desarrollo de los gobiernos, por ende, los CSIRT gubernamentales deben amoldarse a las necesidades del estado o gobierno donde se implementen.

4.1.2.5 CSIRT Militar. Estos equipos de respuesta se centran en los servicios en entidades de carácter militar, profundizando en las capacidades cibernéticas de los servicios de ataque y defensa de una nación. Estos equipos pueden tener un mayor conocimiento en áreas TIC de uso militar o en algunos armamentos.

4.1.2.6 CSIRT Nacional. Estos equipos nacionales juegan un papel de organización nacional y un punto de contacto, ante la presencia de una amenaza o evento de seguridad informática. La función de este CSIRT depende de los roles que se desempeñen, así como de la presencia de otros equipos de respuesta. Podría mencionarse este equipo de respuesta como uno que engloba a los demás equipos dentro de una nación, en donde juega un papel organizativo importante.

4.1.2.7 CSIRT Proveedores. Equipo CSIRT que presta sus servicios a productos relacionados con una empresa de manufactura, estos equipos tienen como propósito mantener al margen problemas de seguridad informática que puedan afectar un producto específico.

4.1.2.8 CSIRT para pequeñas y medianas empresas PYME. Debido a la manera en que se encuentran conformadas estas pequeñas empresas, en muchas ocasiones no se pueden implementar CSIRT en cada una de estas, por lo cual surge la necesidad de la creación de un equipo que sea capaz de cubrir las necesidades a grupos pertenecientes a esta comunidad

4.1.3 Conformación de un CSIRT. Un equipo de respuestas está conformado por uno o varios grupos de expertos que cuentan con las capacidades de ofrecer respuestas oportunas ante un incidente informático, así como la elaboración de planes de recuperación ante incidentes y vulnerabilidades informáticas.

Como cualquier equipo u organización, el CSIRT debe contar con el recurso humano necesario para que pueda atender y ofrecer los servicios para los cuales está dispuesto. Guías como la del Centro Criptológico Nacional de España mencionan que deben contarse con los siguientes roles:

- Un director general o supervisor del equipo CSIRT.
- Personal Técnico que proveerá de los servicios técnicos.
- Investigadores y analizadores de casos o servicios.

Otras Guías, como la de la OEA, mencionan a roles como:

Director: El cual establece las líneas de dirección y organización del equipo de respuesta, así como planifica las estrategias y planes de acción de su equipo a cargo.

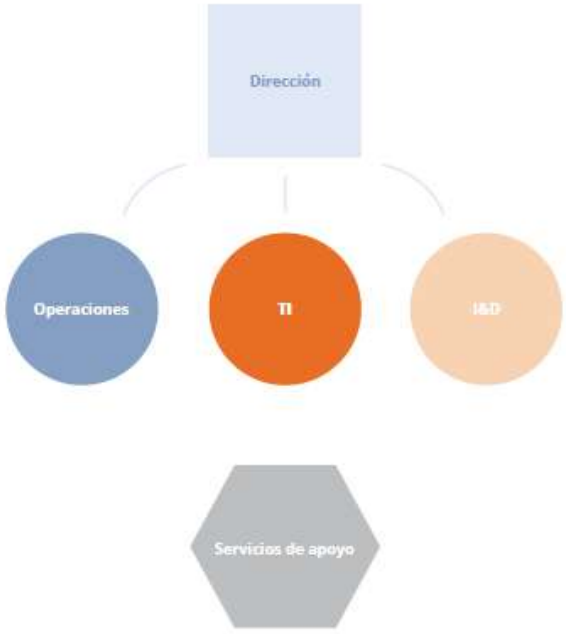
Operaciones: Es el recurso Humano critico de un CSIRT, este quien atiende y gestiona los incidentes reportados. El área de operaciones juega un papel primordial dentro de la organización.

Investigación y Desarrollo: Los integrantes de esta área, tendrán la función de implementar acciones que motiven el desarrollo de nuevas herramientas, de realizar tareas de formación, así como de investigación en áreas de nuevas tendencias tecnológicas y de amenazas cibernéticas.

Implementación y Administración: Esta área y su recurso humano se encargará de administrar los recursos tecnológicos de que dispone el CSIRT. Manejará componentes de infraestructura y tecnológicos como correos electrónicos, sitios web, gestión de solicitudes, servidores, entre otros.

Servicios de Apoyo: Personal que apoya áreas como: prensa, marco legal, administración, finanzas, etc.
Por lo cual se puede resumir la estructura básica de un CSIRT de acuerdo con la figura 1.

Figura 1 Estructura básica CSIRT



Fuente: OEA. Buenas Prácticas para establecer un CSIRT nacional. 2016. 1889 F Street, N.W., Washington, D.C., p. 51

4.1.4 Funciones y perfiles de un CSIRT. Dadas las figuras mencionadas anteriormente el recurso humano de un equipo de respuesta está condicionado a cumplir con los siguientes perfiles y funciones dentro del equipo, los cuales se encuentran recomendados en su implementación de acuerdo con la guía CCN española[3]:

Jefe / director o responsable del equipo.

- Mantener comunicación directa con el equipo.
- Direccionar planes y estrategias.
- Comunicar lo requerido con la comunidad exterior al equipo CSIRT.

Responsable de los sistemas y seguridad de la información.

[3] Centro Criptológico Nacional CCN de España. Op. Cit., p. 18

- Ejecutar procesos de administración y mantenimientos a los recursos TI.
- Análisis de eventualidades (análisis forense y códigos maliciosos).

Responsables de comunicación y relaciones públicas.

- Actividades de comunicación y promoción.
- Identificación de los medios disponibles.
- Mecanismos oficiales de divulgación de información del centro prensa.
- Participación en eventos y foros especializados.
- Afiliación a organismos internacionales.

Responsable de gestión de incidentes.

- La implementación de este dependerá del nivel de servicios por parte del CSIRT.
- Análisis y respuesta a incidentes.
- Soporte a vulnerabilidades.
- Atención a incidencias en dos niveles.

Dentro del proceso de atención, administración y gestión de incidentes de riesgos informáticos, un CSIRT tiene implementados dentro de su estructura niveles de respuesta que están conformados acorde al nivel de complejidad con el que se ha reportado el incidente, lo cual ha groso modo pueden identificarse 2 niveles.

Nivel 1. Nivel de conocimiento técnico básico, el cual cuenta con las capacidades y habilidades para dar respuesta a incidentes en el área TIC. Este nivel debe contar con el conocimiento suficiente para atender y brindar respuesta a incidentes categorizados como frecuentes y que impliquen soluciones técnicas. En casos donde se requiera se deberá establecer comunicación con el nivel 2 si es requerido según la complejidad del incidente.

Nivel 2. Especialista con nivel técnico alto y suficiente para dar respuesta al incidente si es requerido. El personal asociado a este nivel cuenta con conocimientos más avanzados que los ofrecidos en el nivel anterior. En este nivel se deben implementar mecanismos que permitan la comunicación del CSIRT con otros grupos de apoyo que permitan brindar soluciones adecuadas de acuerdo con la complejidad del incidente.

Un nivel o equipo que complementa el cumplimiento de las funciones de atención a incidentes de un CSIRT es el equipo de formación, este ofrece las alternativas para que el personal se encuentre actualizado en las nuevas tecnologías en áreas TI que surjan en el mundo, así como mantener al día al equipo de la presencia de nuevas amenazas, riesgos, antecedentes presentados, con el fin de llevar un registro detallado y tomar las medidas de actuación correspondientes.

4.1.5 Objetivos de un CSIRT. Según E Carozo, C Martinez, L Vidal, G Betarte, A Blanco, E Cota, J Pérez, un CSIRT tiene trazados los siguientes objetivos:

- Realizar un control sobre los incidentes informáticos provocados en una comunidad u organización a la cual se prestan los servicios.
- Estandarizar procesos de comunicación que permiten dirigir y coordinar acciones de respuesta y recuperación ante un ataque malicioso.
- Guardar y recopilar información acerca de cualquier tipo de incidentes presentado en las organizaciones.
- Promover acciones de recuperación de un incidente, identificando las cusas, recolectando evidencia y hallando los responsables de este.
- Ofrecer toda la ayuda necesaria para evitar que se repite el incidente informático.

4.1.6 Servicios CSIRT. Un CSIRT puede ofrecer tres tipos de servicio, los cuales según Agencia Europea de Seguridad de las Redes y de la Información ENISA[4], pueden clasificarse en Servicios reactivos, los cuales cuentan con los servicios básicos a ofrecer por el equipo de respuesta como los análisis de incidentes o la coordinación de respuesta ante los mismos; los servicios Proactivos, dentro de los cuales se realizan las evaluaciones de seguridad y los comunicados al cuerpo CSIRT; Servicios de gestión de calidad de la seguridad, los cuales ofrecen un valor agregado a los servicios reactivos y proactivos, brindando un análisis la evaluación de los riesgos así como una continua capacitación y educación a los miembros del equipo.

Diferentes autores y guías mencionan los servicios que prestan los diferentes CSIRT conformado a nivel internacional, por lo cual en la tabla 1 se observa un

[4] Agencia Europea de Seguridad de las Redes y de la Información, ENISA. Cómo crear un CSIRT paso a paso. [en línea]. [Consulta febrero 12 de 2020]. Recuperado de: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

resumen o compendio de la clasificación de los servicios ofrecidos por estos equipos de respuesta.

Tabla 1. Servicios prestados por un CSIRT

Servicios Reactivos	• *Incidentes.*
	  ○ Servicios de alertas y advertencias ante los incidentes presentados.
	  ○ Tratamiento o gestión de incidentes reportados.
	  ○ Análisis de los incidentes.
	  ○ Respuesta a los incidentes *in situ* (en sitio).
	  ○ Apoyo a las respuestas dadas en los incidentes.
	  ○ Coordinación de las respuestas dadas ante un incidente.
	• *Vulnerabilidades.*
	  ○ Tratamiento y gestión de vulnerabilidades.
	  ○ Análisis de Vulnerabilidades.
	  ○ Respuesta a vulnerabilidades.
	  ○ Coordinación de respuestas ante vulnerabilidades.
	  ○ Asistencia remota ante incidentes o vulnerabilidades.
	• *Herramientas/Artefactos.*
	  ○ Gestión de herramientas.
	  ○ Análisis de herramientas.
	  ○ Respuestas apoyadas con herramientas.
	  ○ Coordinación de respuesta con herramientas.

Servicios Proactivos	• Anuncios y comunicados por parte del CSIRT. • Observación y vigilancia tecnológica. • Auditoria y evaluación de la seguridad. • Configuración y mantenimiento de la seguridad. • Desarrollo de herramientas o aplicaciones para la seguridad. • Prestación de servicios de detección de intrusos. • Divulgación de información con relación a la seguridad informática.
Servicios de Gestión de Calidad de la Seguridad	• Análisis de riesgos. • Planes de recuperación ante un desastre y continuidad del negocio. • Servicios de consultoría en seguridad informática. • Concientización ante la problemática de seguridad. • Educación, formación y capacitación en temas de seguridad. • Evaluación y certificación de productos.

Fuente: William Franco

Descripción de los servicios.

El centro de Coordinación CERT (CERT/CC)[5] realiza una descripción de los servicios de un CSIRT, las cuales se pueden observar en cada una de las categorías mencionadas.

4.1.6.1 Servicios Reactivos. Entre ellos se encuentran:

Alertas y advertencias
Servicio enfocado en emitir las alertas de seguridad ante un intruso o virus informático. Realiza un informe a detalle de la irrupción en sistema, el cual es distribuido al grupo, orientando sobre las medidas y el cuidado que se debe dar al sistema de acuerdo con lo presentado.

Tratamiento de incidentes
Este servicio engloba actividades como recepción diagnostico respuesta ante un reporte del área de comunicación sobre un incidente presentado. A su vez este servicio incluye acciones complementarias como búsqueda y filtrado de la red o algunas correcciones y reparaciones en el área de sistemas.

Análisis de incidentes.
Dentro de este servicio se realiza un examen a la información disponible concerniente al incidente de seguridad reportado, con el fin de averiguar el alcance del incidente, la naturaleza de este, así como las estrategias de que dispone el CSIRT para enfrentarlo.

Respuesta a incidentes *in situ*
Se realiza un enfoque de prestación de servicios en el lugar donde ocurre el incidente, complementando las acciones de comunicaciones a través de líneas telefónicas o asistentes remotos. Este servicio involucra un desplazamiento del equipo al lugar físico donde ocurre el incidente.

[5] Centro de Coordinación CERT. Servicios CSIRT. [en línea]. [Consulta abril 16 de 2020]. Disponible en: http://www.cert.org/

Apoyo a la respuesta a incidentes.
Contrario al servicio que se mencionó anteriormente, el apoyo a la respuesta de incidentes se centra en la ayuda y orientación a través de líneas telefónicas, correo electrónico o asistentes remotos a las víctimas del incidente reportado.

Coordinación de la respuesta a incidentes
Se realiza una coordinación ante las tareas a realizar por parte del equipo de respuesta y las demás partes implicadas en el incidente. En muchos casos estas tareas de coordinación involucran reuniones in situ con la víctima del incidente y expertos del CSIRT.

Tratamiento de la Vulnerabilidad.
Este servicio enfocado en el área de las vulnerabilidades trata de hacer una recopilación de la información acerca de estas a nivel de *hardware* y *software* en medio del análisis de la vulnerabilidad reportada.

Análisis de la vulnerabilidad
Servicios prestados al *hardware* y *software* en busca de aspectos vulnerables dentro del sistema. En gran cantidad de casos se realizan pruebas en búsqueda de las vulnerabilidades que puedan ser explotadas.

Respuesta a la vulnerabilidad
Este servicio establece los parámetros y respuestas adecuadas para mitigar o reparar en su totalidad una vulnerabilidad presentada. Este servicio puede incluir la búsqueda de soluciones provisionales ante una vulnerabilidad.

Coordinación de la respuesta a la vulnerabilidad
El equipo de respuesta deberá notificar a todas las partes de la organización a la que se prestan los servicios la forma de reparar o mitigar las acciones negativas generadas por el incidente. De igual manera se comprueba que la respuesta a la vulnerabilidad explotada se haya aplicado de manera exitosa. En algunas ocasiones en este servicio se requiere la comunicación y coordinación con personal ajeno a la organización o con un CSIRT externo

Comunicados
Además de comunicar a los clientes del CSIRT los desarrollos en el equipo que puedan afectarlos, también se desarrollan procesos de alertas de intrusos o de advertencia acerca de la detección de vulnerabilidades.

Observación de la tecnología
Esta tarea involucra observar los desarrollos técnicos y tecnológicos del mundo digital, así como las actividades y técnicas que implementan los intrusos a la hora de infiltrar un sistema o explotar sus vulnerabilidades

Evaluaciones y auditorias de seguridad
Se realizan estudios, análisis, verificación y auditorías a la infraestructura de la organización, estos basados en los requisitos establecidos por esta o acogiéndose a la normatividad vigente.

Desarrollo de herramientas o aplicaciones para la seguridad
A través de este servicio se orienta de manera segura el uso y mantenimiento de las herramientas o aplicaciones utilizadas por el CSIRT para el desarrollo de sus procesos misionales. Este proceso también puede involucrar los procesos de actualización de las herramientas utilizadas.

Prestación de servicios de detección de intrusos
Cuando este servicio es incluido dentro de un plan de atención, el equipo de respuesta realiza procesos de revisión a los sistemas de detección que existan dentro de una compañía, a partir de allí definen políticas para atender a eventos que superen el umbral de configuración definido para afrontar amenazas.

Divulgación de información con relación a la seguridad informática.
A través de este servicio se le proporciona al grupo de clientes del CSIRT, herramientas e información útil acerca de temas relacionados con seguridad informática y que estos pueden implementar.

Análisis de riesgos.
Este proceso da un valor agregado y de mayor profesionalismo a los CSIRT, a través de la evaluación cualitativa y cuantitativa de los riesgos activos en una organización, permite a esta ofrecer estrategias de protección más eficientes.

4.1.7 Planes de recuperación ante un desastre y continuidad del negocio. A través de acciones de planificación acorde a las experiencias adquiridas en el CSIRT, se pueden crear diferentes planes de respuesta, recuperación y gestión de desastres.

Servicios de consultoría en seguridad informática
A través de este servicio un CSIRT puede asesorar a una organización acerca de las mejores prácticas a implementar dentro de una organización, de esta manera puede intervenir o aconsejar sobre la compra y adquisición de infraestructura tecnológica a nivel de hardware y software de una empresa.

Concientización ante la problemática de seguridad
Gracias a la sensibilización y concientización ejercida dentro de los clientes CSIRT, se puede hacer que las labores de gestión diarias del equipo se ejecuten de forma más segura. De esta manera se logra que el índice de incidentes o ataques informáticos descienda considerablemente dentro de la organización.

Educación, formación y capacitación en temas de seguridad
A través de este servicio se ofrecen a los clientes del CSIRT, herramientas de capacitación, en donde a través de folletos, seminarios, conferencias, cursos y tutoriales; información que les permita implementar acciones seguras dentro del desarrollo laboral que como organización llevan.

Evaluación y certificación de productos
Por medio de este servicio, se realizan labores de evaluación a las herramientas y aplicaciones utilizadas dentro de la organización, estas pueden ser herramientas de código libre o de carácter comercial.

4.2 MARCO CONCEPTUAL

4.2.1 Seguridad Informática y seguridad de la información. Aunque estos dos términos suelen confundirse con gran facilidad, se debe mencionar que ambos buscan o cumplen el mismo objetivo estos se aplican de diferente forma.
La seguridad informática está relacionada o encaminada a la protección de la infraestructura tecnológica de carácter informático que guarda o transmite información a través de redes de datos y telecomunicaciones. Entre estas se encuentran los tipos Físicos, para proteger de amenazas del medio o entorno, como

incendios e inundaciones; lógicos, que protegen la seguridad lógica del sistema, como la encriptación. De igual manera dependiendo del momento en que se da la protección como la seguridad activa o preventiva, que evitan las amenazas antes de que se produzcan y la seguridad pasiva o correctivas que minimizan las consecuencias de fallas de seguridad.

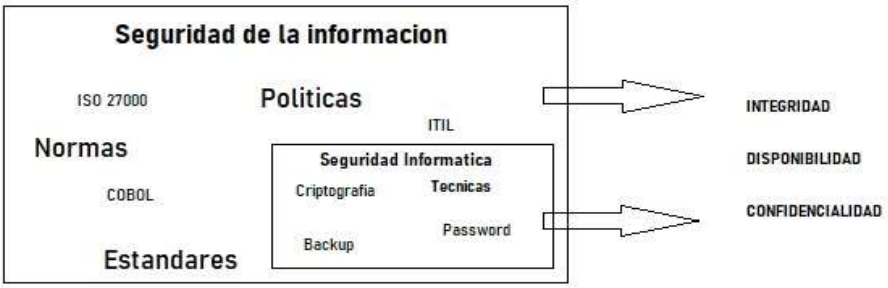
La seguridad de la información reúne los conjuntos de técnicas y procedimientos encaminados a proteger la información en tres instancias (o pilares de la información).

- Integridad, información completa y correcta.
- Disponibilidad, uso de la información en cualquier momento.
- Confidencialidad, uso de la información solo al personal interesado o autorizado. Alejado de terceros.

De esta manera se puede inferir que la seguridad informática es un concepto particular de un concepto general como es el de la seguridad de la información o se puede mencionar a la seguridad informática, como una rama de la seguridad de la información que está encaminada a la protección de infraestructura física (*hardware*) como lógica (*software*) dentro de los sistemas informáticos.

Dicho en otras palabras, la seguridad informática se encuentra basada en procesos técnicos y tecnológicos, los cuales difieren de los procesos de gestión, normativos y políticos en los cuales se basa la seguridad de la información.

Figura 2. Relación seguridad de la información - Seguridad informática



Fuente: Propia del autor

4.2.2 Normas y estándares en Seguridad Informática. La seguridad en los sistemas informáticos cada día toma niveles más críticos, tomado en consideración el crecimiento exponencial de redes como internet y los servicios web soportados sobre esta, obligando a aunar esfuerzos internacionales para que existan medidas

en pro de mantener seguros, íntegros y protegidos los diferentes sistemas de información.

En este orden de ideas surgen en la labor diferentes organismos internacionales que tiene como intención implementar normas, medidas y procedimientos regulados, los cuales buscan hacer que las actividades informáticas cumplan con ciertas condiciones de uso de información y tratamiento de esta para preservar la integridad, disponibilidad y confidencialidad de los datos. Organismos como la ISO (*International Organization for Standardization*) es una entidad que se dedica a la creación de normas o estándares para asegurar la calidad, seguridad y eficiencia de productos y servicios en varios ámbitos organizacionales entre estos el de la seguridad informática.
Dentro de la labor realizada por la ISO en el área de seguridad informática, se encuentra publicada la normatividad estandarizada bajo la denominación de ISO/IEC 27000, la cual es un conjunto de estándares que buscan establecer buenas prácticas para la gestión de la seguridad de la información y los sistemas de gestión de seguridad de la información (SGSI). Este conjunto de estándares esta constituidos por diferentes normas que buscan la seguridad de la información (27001 - 27799). Los pilares de este estándar son las normas ISO/IEC 27001 como norma estandarizada para la seguridad de la información, la cual establece los requisitos necesarios para establecer un SGSI. Esta norma se divide en dos partes, una para la evaluación de riesgos y la otra para la implementación de medidas de seguridad. Norma ISO/IEC 27002, la cual se establece como estándar o norma internacional que ofrece un código de buenas y mejores prácticas para la implementación de Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones.

De igual manera, existen gran cantidad de conceptos asociados a la seguridad informática, algunos de ellos dan claridad sobre temas de análisis y gestión de riesgos propios de las actividades diarias desarrolladas por equipos de respuesta ante incidentes informáticos, por lo cual se tratarán los más relevantes a continuación.

4.2.3 Activo de Información. Son todos los recursos que tienen un valor medible dentro de una organización.

4.2.4 Análisis de Riesgos. Metodología que sirve para identificar y evaluar probables daños y pérdidas a consecuencia del impacto de una amenaza sobre un sistema.

4.2.5 Amenaza. Evento que puede causar algún tipo de accidente informático dentro de una organización, alterando o degradando sus activos.

4.2.6 COBIT. Objetivos de control para la información y tecnologías relacionadas por sus siglas en ingles Control *Objectives for Information and related Technology*, es un marco de buenas prácticas o conjunto de normas para la gestión dirigidas a la organización de las tecnologías de la información TI en el sector empresarial.

4.2.7 Confidencialidad, propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información

4.2.8 Control de acceso, conjunto de métodos los cuales contribuyen a la gestión de acceso por parte de los usuarios ya sea a un sistema informático o un sistema físico.

4.2.9 Evaluación del riesgo, proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

4.2.10 Gestión del Riesgo, actividades encaminadas a dirigir y controlar una organización de TI en situaciones relacionadas con el riesgo.

4.2.11 Incidente de seguridad, ocurrencia de un evento dentro de la organización TI, que pone en riesgo la integridad, disponibilidad o confidencialidad de la información.

4.2.12 Información, conjunto de datos estructurados y organizados que dan valor a una organización

4.2.13 Integridad, propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción de esta.

4.2.14 Políticas, conjunto de normas establecidas dentro de la organización para dar cumplimiento a un proceso o procedimiento.

4.2.15 Riesgo, es la posibilidad de que se produzca una acción que ponga en peligro los activos de la organización TI.

4.2.16 Seguridad Informática, área o disciplina que se encarga de conservar y proteger la integridad disponibilidad y disponibilidad de la información.

4.2.17 Servicios Proactivos, actividades encaminadas dentro de un CSIRT, para brindar información que contribuya a la protección de la infraestructura tecnológica.

4.2.18 Servicios Reactivos, actividades encaminadas a responder ante un evento de seguridad indeseado, reportado por algún miembro del equipo CSIRT, servicios principales del componente CSIRT.

4.2.19 Vulnerabilidad, Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

4.3 ANTECDENTES O ESTADO ACTUAL

A raíz de la presentación de incidentes informáticos, surge la necesidad de hacer frente o la creación de mecanismos de respuesta que permitan ofrecer una solución eficaz a los problemas de seguridad informática. Se hace necesario que existan organizaciones capaces de analizar un incidente para formular métodos o técnicas que prevengan los mismos y se permitan bajo un análisis dar soluciones adecuadas. Bajo esta premisa surgen los equipos de respuesta ante incidentes informáticos CISRT, los cuales viene siendo conformados hace alrededor de 30 años, debido a la necesidad de hacer frente a amenazas informáticas que se esparcieron en la red de internet, una red en construcción conocida como ARPANET, en la década de los 80-90, en donde el “gusano Morris” fue liberado causando un gran revuelo y un cambio radical en la seguridad informática[6].

Los CSIRT contribuyen al proceso de gestión de riesgos y de seguridad de información, los cuales se apoyan en diferentes leyes y regulaciones internacionales para proteger la información y evitar el crecimiento de las amenazas.

En la actualidad existen a nivel internacional gran cantidad de equipos de respuesta conformados en diferentes áreas o ámbitos de actuación, los cuales ofrecen servicios tanto de prevención, como de acción contra los incidentes informáticos,

[6] Welivesecurity. Martes de retrospectiva: el gusano Morris. [en línea]. [Consulta: octubre 5 de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris/

estos últimos denominados como servicios reactivos dentro del equipo de incidentes informáticos. Países como estados unidos, Venezuela, Uruguay, Panamá, Colombia, Brasil, Argentina, entre otros, cuentan con equipos de respuesta que son capaces de realizar labores de gestión de riesgo y ofrecer soluciones pertinentes ante un incidente informático reportado. Dentro de algunos CSIRT se pueden mencionar:

América

- US-CERT, *United States Department of Homeland Security*
- CERT *Coordination Center*, Carnegie Mellon University
- UNAM CERT, Mexico
- CERT.br, Brazil,
- colCERT, Grupo de Respuesta a Emergencias Cibernéticas de Colombia,
- Ar-CERT, Argentina,
- Venezuela CERT/VENCERT,
- CSIRT CHILE, Chile
- CLCERT, Chile
- CSIRT BANELCO, Argentina
- CERTuy, Uruguay

Europa

- CERT-EU
- Ai CERT
- PRACE CSIRT
- CSIRT-ECB
- ESACERT

De la misma manera en que se ha conformado diferentes equipos de respuesta a incidentes de carácter global, existen en la web u otras fuentes literarias guías que ofrecen al lector una perspectiva completa para establecer en una organización un equipo con las características y requerimientos necesarios para ofrecer un apoyo a la seguridad informática. La organización de los estados americanos OEA y gracias al apoyo financiero de Canadá, ofrece una guía de buenas prácticas para establecer CSIRT de carácter nacional, esta guía emitida en abril de 2016 cuenta con apartados de planeación, ejecución y cierre de un CSIRT, los cuales fueron de variedad utilidad para el desarrollo del documento actual, en donde se toman como

referencia las guías de planeación y selección del tipo de CSIRT, así como los perfiles y experiencia profesional requerida para la conformación del CSIRT de la empresa “Platino Sistemas”.

Otras guías de implementación como la del centro criptológico nacional de España a través del CCN-CERT que tienen conformado y la guía de creación de un CSIRT paso a paso, autoría de Agencia Europea de Seguridad de las Redes y de la Información (ENISA) han servido como apoyo para la revisión de los tipos de servicio que ofrece un CSIRT, así como el personal profesional que los conforman, para que en este documento se formulen y se precisen los perfiles profesionales adecuados.

En conjunto con las guías de creación y la documentación existente con la presencia de equipos de respuesta a nivel mundial, se ha optado por realizar un análisis sistemático de la información existente en el territorio colombiano acerca de equipos de respuesta a incidentes informáticos, así como la normativa que rige la seguridad de la información, con lo cual se establecieron las formas legales que sustentan las actividades informáticas, tales como el CONPES 3701, la ley 1273 de 2009 y algunos artículos de la constitución política colombiana en pro de la seguridad de la información. Este Marco legal permite crear y fundamentar las políticas operacionales del CSIRT propuesto en este documento, así como la normatividad y estándares vigentes de la norma ISO/IEC 27001:2013, estándar base para el modelo integrado de calidad del CSIRT en la organización “Platino Sistemas”.

4.4 MARCO LEGAL

4.4.1 Normativa Nacional. El gobierno nacional colombiano ha implementado medios, mecanismos y normatividad que tiene como fin regular e impartir lineamientos políticos para la ciberseguridad y ciberdefensa en la nación. Estos lineamientos son mencionados en el Documento CONPES 3701 el cual fue publicado durante el año 2011, el cual menciona como objetivo general “Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa), creando un ambiente y unas condiciones para brindar protección en el ciberespacio.”

El documento CONPES 3701 fue publicado con el fin de dar a conocer los lineamientos de política en ciberseguridad y ciberdefensa, los cuales tienen un

enfoque estratégico nacional que buscan contrarrestar el incremento de las amenazas cibernéticas que puedan afectar de manera significativa al país. El documento recoge los antecedentes nacionales, en medio de los cuales se menciona normativa institucional colombiana como los fundamentos constitucionales en torno a la seguridad digital mencionados en el artículo dos estableciendo el "fin esencial del Estado la promoción de la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución" ; De igual manera se habla sobre los derechos y deberes ciudadanos en torno a la seguridad de los datos y utilización del espacio electromagnético en los artículos 15, 76 y 101 de la constitución política así:

Artículo 15 capitulo 1 de la constitución política, donde se cita

> Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
> La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.
> Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.[7]

Artículo 76 capitulo 2 de la constitución política, donde se cita

> Artículo 76. La intervención estatal en el espectro electromagnético utilizado para los servicios de televisión estará a cargo de un organismo de derecho público con personería jurídica, autonomía administrativa, patrimonial y técnica, sujeto a un régimen legal propio[8].

Artículo 101 capítulo 4 del territorio, Titulo III de la constitución política, donde se cita

> Artículo 101. Los límites de Colombia son los establecidos en los tratados internacionales aprobados por el Congreso, debidamente ratificados por el presidente de la República, y los definidos por los laudos arbitrales en que sea parte la Nación. Los límites

[7] COLOMBIA. CONSTITUCIÓN POLÍTICA DE COLOMBIA. (1991). De los derechos fundamentales. Título II, Capitulo 1, Artículo 15
[8] COLOMBIA. CONSTITUCIÓN POLÍTICA DE COLOMBIA. (1991). De los Derechos Fundamentales. Título II, Capitulo 2, Artículo 76

> señalados en la forma prevista por esta Constitución sólo podrán modificarse en virtud de tratados aprobados por el Congreso, debidamente ratificados por el presidente de la República.
>
> Forman parte de Colombia, además del territorio continental, el archipiélago de San Andrés, Providencia y Santa Catalina, la isla de Malpelo, además de las islas, islotes, cayos, morros y bancos que le pertenecen.
>
> También son parte de Colombia, el subsuelo, el mar territorial, la zona contigua, la plataforma continental, la zona económica exclusiva, el espacio aéreo, el segmento de la órbita geoestacionaria, el espectro electromagnético y el espacio donde actúa, de conformidad con el Derecho Internacional o con las leyes colombianas a falta de normas internacionales.[9]

De igual manera el Gobierno nacional colombiano ha establecido procedimientos penales los cuales dictan a través de la ley 1273 de 2009[10] en el artículo 269A - 269J, los delitos asociados a la protección de la información y de los datos y las sanciones que acarrean

4.4.2 Ley 1273 DE 2009. Ley que modifica el código penal colombiano y se crea bien jurídico para la protección de la información y de los datos.

CAPITULO I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático, quien ingrese a un sistema informático sin la autorización necesaria por el propietario de este, incurrirá en un apena de prisión que va de 48 a 96 meses y una multa de 100 a 1000 SMLMV.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación, quien ingrese a una red o sistema informáticos y obstaculice o impida el normal funcionamiento del mismo, incurrirá en una pena de prisión que va de 48 a 96 meses y una multa de 100 a 1000 SMLMV.

[9] COLOMBIA. CONSTITUCIÓN POLÍTICA DE COLOMBIA. (1991). De los Extranjeros. Título III, Capitulo 4, Artículo 101

[10] COLOMBIA SECRETARIA SENADO, ley 1273 2009, [en línea]. [Consulta abril 10 de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Artículo 269C: Interceptación de datos informáticos, quien sin orden judicial realice la interceptación de datos tomada de una red telemática o sistema informático incurrirá en un apena de prisión que va de 36 a 72 meses.

Artículo 269D: Daño Informático, quien realice daños a los sistemas informáticos y a la información allí contenida incurrirá en una pena de prisión que va de 48 a 96 meses y una multa de 100 a 1000 SMLMV.

Artículo 269E: Uso de software malicioso, el que haga uso de software mal intencionado en territorio nacional y cause daños a los sistemas informáticos, incurrirá en una pena de prisión que va de 48 a 96 meses y una multa de 100 a 1000 SMLMV.

Artículo 269F: Violación de datos personales, quien manipule información personal de otras personas obtenida de los archivos de información, como bases de datos, y la utilice para beneficio propio incurrirá en una pena de prisión que va de 48 a 96 meses y una multa de 100 a 1000 SMLMV.
Artículo 269G: Suplantación de sitios web para capturar datos personales, quien de manera mal intencionada y fraudulenta haga uso de técnicas para suplantar páginas web, correos electrónicos y realice cambios de dominios o suplantación de IPs, incurrirá en una pena de prisión que va de 48 a 96 meses y una multa de 100 a 1000 SMLMV.

CAPITULO II. De los atentados informáticos y otras infracciones

Articulo 269I: Hurto por medios informáticos y semejantes, quien haciendo uso de sistemas informáticos hurte información relevante para terceros y obtenga provecho de ello, incurrirá en una pena de prisión de seis (6) a catorce (14) años.

Artículo 269J: Transferencia no consentida de activos, quien haciendo uso de sistemas informáticos, realice la manipulación de activos en actos como transferencias y sean perjudiciales para un tercero, incurrirá en pena de prisión de 48 a 120 meses y en multa de 200 a 1.500 SMLMV**.**

4.4.3 Normativa Internacional. A nivel internacional existen varios instrumentos que cuentan con una relación en seguridad digital importante, dentro de los cuales se encuentran los mencionados a continuación:

Convenio sobre Ciberdelincuencia del Consejo de Europa, convenio mediante el cual se adoptan las medidas pertinentes para facilitar acciones que prevengan conductas delictivas, además de proporcionar herramientas penales eficientes en el tratamiento y detección de conductas antijuridicas[11].

Resolución AG /RES 2004 (XXXIV-O/04) Asamblea General de la OEA, resolución que crea estrategias que combaten las amenazas en el ámbito de la seguridad informática con enfoques multidimensionales y disciplinarios, los cuales están encaminados a crear una cultura de seguridad cibernética en la comunidad[12].

Dentro del marco legal internacional destaca la declaración realizada por la OEA en la quinta sesión plenaria llevada a cabo el 20 de marzo de 2015[13] en donde se da desarrollo a un proyecto capaz de brindar asistencia técnica a los estados americanos miembros de la OEA y que les permita la creación de un listado donde se mencione el tipo de infraestructura crítica y realizar la clasificación de la misma, con el fin de mejorar la evaluación de las vulnerabilidades riesgos y amenazas tecnológicas que puedan sufrir.

4.5 MARCO ESPACIAL

Platino Sistemas es una empresa colombiana que se encuentra ubicada en la ciudad de Bogotá D.C. la cual ofrece a sus clientes servicios de seguridad para la protección de información. Esta empresa se ha trazado como meta crear un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT para el año 2022, el cual beneficiara a sus clientes de acuerdo con un tipo de servicio contratado.

Platino sistemas tiene un cubrimiento en sus servicios de seguridad informática a nivel nacional, por lo cual se verá beneficiada toda la población colombiana que desea obtener sus servicios.

---

[11] Council Of Europe. Serie de tratados europeos. Convenio Sobre la Ciberdelincuencia. [en línea]. [consulta: abril 17 de 2020] Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[12] Departamento de derecho internacional OEA. Resolución asamblea general. AG/RES. 2040 (XXXIV-O/04). [en línea]. [Consulta: abril 17 de 2020]. Disponible en: http://www.oas.org/juridico/spanish/ag04/agres_2040.htm

[13] OEA. comité interamericano contra el terrorismo (CICTE). Declaración protección de infraestructura crítica ante las amenazas emergentes. [en línea]. [Consulta: abril 17 de 2020]. Disponible en: https://www.oas.org/en/sms/cicte/documents/sessions/2015/CICTE%20DOC%201%20DECLARACION%20CICTE00955S04.pdf

Actualmente la empresa ofrece servicios de carácter presencial y personal en las principales ciudades del país y espera a través de la creación del equipo de respuesta a incidentes informáticos, brindar apoyo remoto a localidades más apartadas del país en donde a través de diferentes medios y con el apoyo de Tecnologías de la Información, brindar soluciones ante incidentes informáticos.

4.6 MARCO METODOLOGICO

La recopilación y revisión de literatura permite adoptar conceptos para amoldar la idea de un proyecto en cualquier campo o disciplina profesional, con lo cual se brindará un apoyo en diferentes referentes y autores para elaborar una idea propia.

Según Kitchenham,[14] "Una revisión sistemática es una manera de evaluar e interpretar toda la investigación disponible, que sea relevante respecto de una interrogante de investigación particular, en un área temática o fenómeno de interés".

Por lo cual Kitchenham, define un método sistemático que permite realizar la revisión de varias fuentes bibliográficas y literarias con el fin de obtener unos resultados esperados de un tema en concreto. Este método se divide en tres etapas:

- Planificación de la revisión, etapa en donde se identifica la necesidad de la revisión y la definición de protocolos para la misma.
- Desarrollo de la revisión; etapa en la cual se realiza una búsqueda y selección de estudios primarios.
- Publicación de los resultados.

Gracias a metodologías como la descrita anteriormente, se podrá dar desarrollo a este y muchos otros proyectos, los cuales requieren de revisión, análisis y comparación de muchas teorías, literatura, estándares y normatividad para obtener los resultados deseados.

El diseño del documento que permitirá especificar el ámbito, creación, los servicios, la estructura, perfiles, políticas y procedimientos de un Centro de Respuesta a Incidentes Cibernéticos CSIRT para la empresa Platino Sistemas, estará

[14] KITCHENHAM, B., (2004) Procedures for Performing Systematic Reviews, TR/SE-0401, Keele University.

fundamentado en la metodología de indagación, análisis y consulta de un gran compendio de documentación que permita revisar, evaluar y comparar diferentes modelos a nivel nacional e internacional sobre la implementación de estos centros de respuesta en diferentes ámbitos laborales, académicos y comerciales.

Por medio de la diferente documentación existente acerca de la conformación y estructura de un equipo de respuesta ante incidentes informáticos se podrán definir las mejores estrategias o recomendaciones para definir la estructura orgánica del CSIRT en la proyección para su implantación en la empresa Platino Sistemas, así como la definición puntual de los servicios proactivos, reactivos y complementarios que se presentarán en el catálogo del CSIRT.

A su vez se sustentará la creación de las políticas y procedimientos operacionales del equipo de respuesta en la normatividad proporcionada por el estándar ISO/IEC 27001:2013 el cual menciona controles del tratamiento de la información en los anexos del estándar en su versión más actual.

5. RESULTADOS

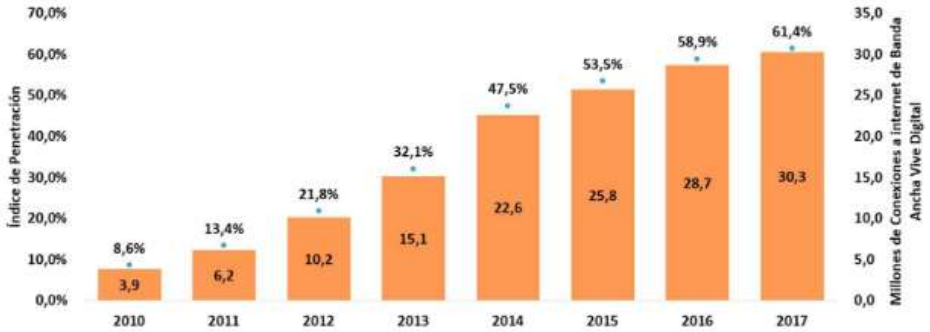
5.1 PANORAMA ACTUAL DE CIBERSEGURIDAD EN COLOMBIA.

Colombia es un país que se encuentra en constante crecimiento en una gran cantidad de aspectos; comerciales, laborales, gubernamentales, de salud, tecnológicos e informáticos, entre otros. Con lo cual se busca estar a la vanguardia y de acuerdo con los niveles de desarrollo mundiales, buscando así, estar a la par de lo exigido por un mundo globalizado.

Un aspecto en el que se centra su crecimiento es el informático, donde día a día se toman medidas que fomenten el crecimiento de la nación con respecto al mundo tecnológico, a su vez se ha implementado infraestructura que otorga mayor cobertura en el área TI dentro del país, por ejemplo, en el acceso a internet.

Diferentes fuentes han realizado análisis y estudios sobre el cubrimiento de internet en Colombia, tal es el caso de la revista Dinero, en donde se menciona a través de un artículo tecnológico, que la nación ha incrementado en alrededor de un 70% las conexiones a internet en tan solo ocho años[15], con lo cual han afirmado que alrededor del 64% de los hogares y un 68% de las empresas cuentan con acceso a internet. Por lo anterior existen más de 30.5 millones de conexiones de internet de banda ancha en la región.

Grafica 1. Índice de penetración y número de conexiones a internet Banda Ancha



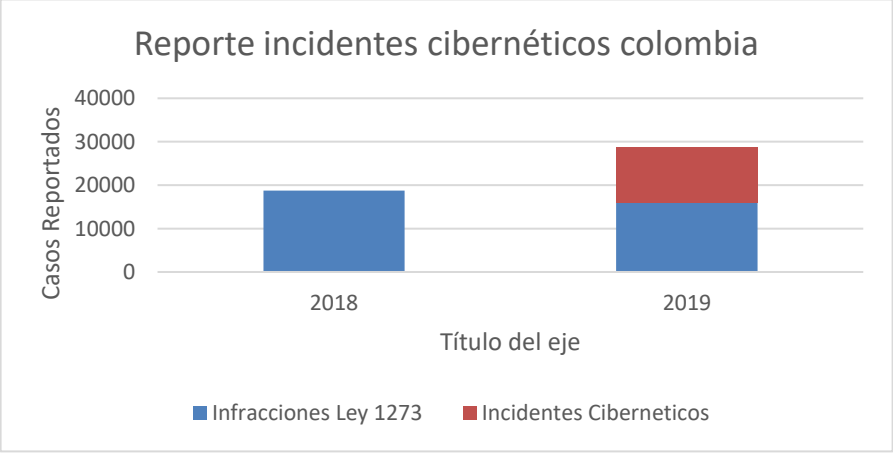
Fuente: Portal oficial de estadísticas del sector TIC – Colombia. Disponible en: www.colombiatic.mintic.gov.co

[15] Dinero. Colombia incremento en un 70% sus conexiones a internet en ocho años. [en línea]. [Consulta: 23 de abril de 2020]. Disponible en: https://www.dinero.com/pais/articulo/balance-conexiones-a-internet-en-colombia-2010-2008/260104

De la misma manera que ha crecido la cobertura de este tipo de conectividad en el ambiente colombiano, también han crecido las demandas y denuncias relacionadas con temas de incidentes informáticos, en donde se reportan ante las autoridades colombianas casos de suplantación de identidad, recepción de correos electrónicos fraudulentos (*phishing*) o simples sucesos de infección a través de páginas web; Clonación de tarjetas de crédito y débito, entre otros y es que como lo afirma "certicamara", empresa de certificación colombiana, las principales ciudades del país concentran más del 70% del ciber crimen nacional, debido a que ciudades como Bogotá, Medellín, Cali o Cartagena cuentan con un gran alcance tecnológico y acceso a internet[16], con lo cual se confirma la situación planteada; a mayor capacidad de conexión, mayor reporte de delitos informáticos.

Durante el año 2019 se han incrementado los reportes de delitos cibernéticos ante las autoridades dispuestas por el gobierno nacional, en donde organismos e investigadores del Tanque de Análisis y creatividad de las TIC (TicTac), la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional, mediante un estudio realizado ante las tendencias del Cibercrimen en Colombia, mencionan que hubo un incremento del 54% con respecto al año 2018, lo que conlleva a la identificación de alrededor de 29 mil casos delictivos, de los cuales alrededor del 55% fueron reportados con infracciones directas a la ley 1273 de 2009.

Grafica 2. Reportes incidentes cibernéticos Colombia.

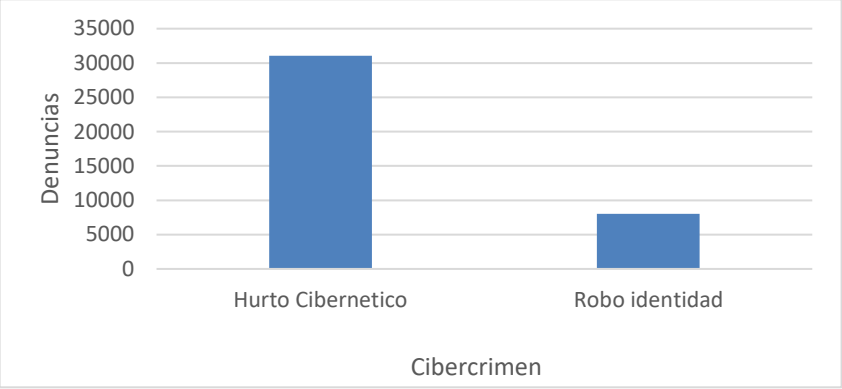


Fuente: Propia del autor.

[16] Certicamara. S.A. SEGURIDAD INFORMÁTICA CERTICÁMARA S.A. Panorama del Cibercrimen en Colombia. [en línea]. [Consulta: abril 24 de 2020]. Disponible en: http://blogs.portafolio.co/seguridad-informatica-certicamara-sa/panorama-del-cibercrimen-colombia/

A través de este reporte que fue compartido por el diario El tiempo[17], se encontró que del año 2017 a octubre de 2019 se hicieron en total 52.901 denuncias referentes a cibercrímenes de las cuales los hurtos que se realizan a través de medios informáticos se reportaron 31.058, en segundo lugar, el robo de identidad con 8.037 reportes.

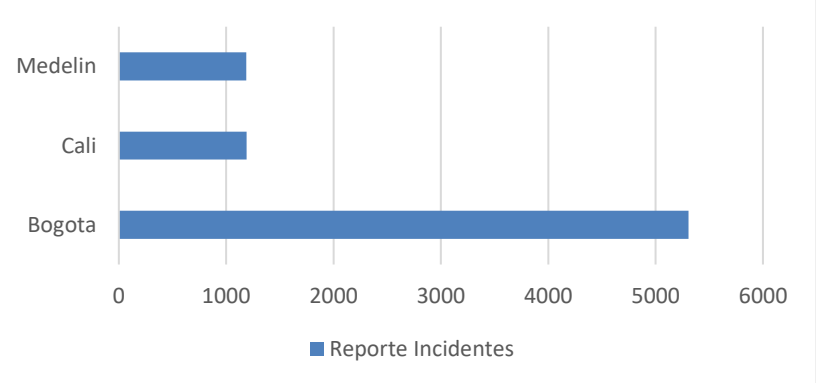
Grafica 3. Reporte Denuncias al Cibercrimen



Fuente: Propia del autor.

Dentro de las principales ciudades del país, Bogotá fue la ciudad que más incidentes reportó (5.308), luego Cali (1.190) y Medellín (1.186).

Grafica 4. Reporte Denuncias al Cibercrimen

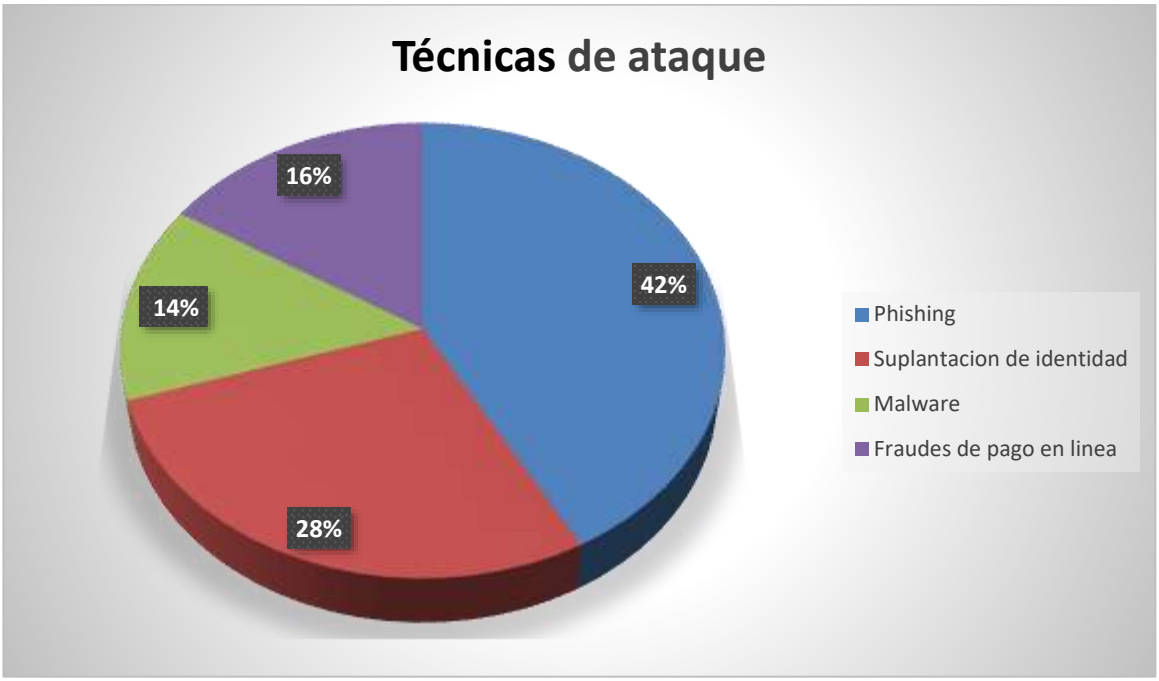


Fuente: Propia del autor.

[17] El Tiempo. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. [en línea] [Consulta: abril 24 de 2020]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

Para el año 2019, el estudio realizado por el TicTac, el CCIT y el C4 de la Policía Nacional [18] señala que el principal motivo para efectuar ciber crímenes es el económico, así como señalan las diferentes técnicas utilizadas por los atacantes, resumidas en la gráfica 5.

Grafica 5. Técnicas de ataque



Fuente: Propia del autor

De igual manera en que se realizan reportes por parte de la ciudadanía Colombia, las empresas de diferentes sectores de producción, también reportan haber sido afectadas por los cibercriminales, en donde se detectan técnicas de acceso a sistemas informáticos ligadas a la ingeniería social, logrando así suplantar identidades y robando información confidencial.

5.1.1 Consejo Nacional de Política Económica y Social, Política Nacional de Seguridad Digital. Gracias al crecimiento tecnológico del país, la república de Colombia a través del Consejo Nacional de Política Económica y Social CONPES ha publicado un documento en el cual se realiza un enfoque a las áreas de ciberseguridad y ciberdefensa de la nación. Este documento corresponde al

[18] Ibid.

CONPES 3701 el cual dicta lineamientos de política para contrarrestar y mitigar los efectos de las amenazas cibernéticas en el entorno digital nacional. El documento ha logrado implementar una institución en el país referente a la seguridad digital e informática, así como posicionar al país como referente internacional en áreas que rodean a la ciberseguridad y a la ciberdefensa[19]

A través del CONPES 3701, el gobierno colombiano buscó fortalecer la capacidad de respuesta de la nación contra diferentes incidentes informáticos, en donde se buscó un ambiente propicio para brindar la protección necesaria. Para lograr este gran objetivo se apoyaron en acciones como la implementación de instancias que prevenían y coordinaban respuestas frente a amenazas cibernéticas, realizar jornadas de capacitación en temas referentes a ciberseguridad y fortalecer el área legislativa en materia de seguridad informática.

Creación de instancias como respuesta ante incidentes informáticos.

Gracias a la política de ciberseguridad y ciberdefensa instituida en la nación, se han institucionalizado organismos que dan solución al tema, donde se ha dado paso a la creación de instancias como:

- El Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional,
- El Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia
- El Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia,
- El Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL),
- La Delegatura de protección de datos en la Superintendencia de Industria y Comercio.
- La Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones
- El Comité de ciberdefensa de las Fuerzas Militares
- La Comisión Nacional Digital y de Información Estatal, mediante el Decreto 32 de 2013 del Ministerio de Tecnologías de la Información y las

[19] PLANEACIÓN, DEPARTAMENTO NACIONAL DE, Ministerio de Tecnologías de la Información y las Comunicaciones, S. de I. y C. (2018). POLÍTICA NACIONAL DE EXPLOTACIÓN DE DATOS (BIG DATA). P. 9

Comunicaciones, por él cual se crea la Comisión Nacional Digital y de Información Estatal[20].

Gracias a la creación de estas entidades el estado colombiano ha logrado mantenerse a nivel mundial como una nación que se encuentra dentro de los primeros países en la lucha contra el cibercrimen, adoptando las medidas necesarias para frenar su crecimiento, así como la mitigación al riesgo por la presentación de algún cibercrimen o reporte de incidente en el área.

A través del documento CONPES 3701, los ministerios de TIC, defensa nacional, de educación, del interior, justicia y derecho, relaciones exteriores, así como algunos entes administrativos de la nación; hicieron algunas recomendaciones al Consejo Nacional de Política Económica y Social, dentro de las cuales destacan:

- Elaborar planes para fortalecer la infraestructura física y tecnológica de colCERT, del CCP y del CCOC, para el mes de diciembre de 2019.

- Actualizar de manera periódica el inventario de estructuras criticas cibernéticas de la nación.

- Diseñar modelos para la gestión de riesgos de seguridad digital a nivel nacional donde se defina un plan estratégico de cooperación y colaboración en el ámbito nacional en temas de seguridad digital.

- Solicitar al ministerio de educación crear contenidos relacionados a la gestión de seguridad digital.

- Adoptar a partir del año 2018, un modelo de gestión de riesgos de seguridad digital.

5.1.2 Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT. Siguiendo las recomendaciones dadas por documentos como el CONPES 3701, así como la atención a necesidades por parte de la nación en materia de seguridad informática, se crearon organismos para atender llamados y brindar respuestas ante amenazas cibernéticas, tal es el caso de colCERT, un equipo de respuesta ante incidentes informáticos en la republica colombiana.

[20] Ibid. Institucionalidad. p. 14

Como lo citó su sitio web oficial:

> colCERT, tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional[21].

De igual manera colCERT tiene trazados ciertos objetivos para prestar el servicio de ciberseguridad en el país, dentro de los cuales se destacan el ofrecer servicios de prevención ante incidentes informáticos, actuar como punto de comunicación a nivel internacional con otros equipos de respuesta y el desarrollo de protocolos de respuesta ante un incidente informático presentado. Para aquellas personas que deseen realizar un reporte de un incidente informático deben seguir las recomendaciones dadas por parte de colCERT, la cuales pueden ser verificadas desde el sitio web oficial[22]

Tener presentes los tipos de incidentes a reportar

- Intentos de acceso no autorizado
- Denegación de servicios.
- Uso no autorizado de un sistema informático.

A su vez los reportes de incidentes realizados ante colCERT deberán especificar la fecha y hora exacta del evento, así como proporcionar un contacto (correo electrónico, número telefónico, entre otros) y la información detallada de lo ocurrido. colCERT juega un papel muy importante en el ámbito de desarrollo digital de Colombia, este se encarga de llevar datos de carácter informativo que buscan crear planes de actuación ante nuevos reportes de incidentes informáticos, los cuales se ajustan a las tendencias por parte de los cibercriminales y las técnicas que utilizan. De esta manera el equipo de respuesta de manera periódica revisa el panorama de seguridad digital del país en donde se pueden analizar algunos ataques a nivel nacional e internacional.

[21] COLCERT. Nuestra misión. [en línea]. [Consulta: abril 25 de 2020]. Disponible en: http://www.colcert.gov.co/?q=acerca-de
[22] http://www.colcert.gov.co

Panorama cibernético colombiano según colCERT

Para el mes de abril de año 2019, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, a cargo de su coordinador Wilson Prieto, realizaron un análisis de los ataques realizados durante el año 2018 y 2019[23], en donde se puede observar que durante el año 2018 se perpetuaron ataques a la banca, organizaciones de encomiendas y mensajería, así como algunas universidades.

colCERT realizo la entrega mediante cifras de la gestión de incidentes reportados durante 2018, los cuales pueden observarse en la gráfica 6.

Grafica 6. Incidentes gestionados colCERT 2018

CLASIFICACION DE LOS CIBERINCIDENTES	PORCENTAJE
Intrusiones - Defacement	43,0 %
Obtención de información - Phishing	16,1 %
Código Dañino - Malware	14,6 %
Intrusiones - Explotación Vulnerabilidad	10,2 %
Intrusiones - Compromiso Aplicación	6,8 %
Criptojacking	4,7 %
Disponibilidad - Denegación [Distribuida] del Servicio DoS / DDoS	1,3 %
Intrusión-Ataque de fuerza bruta	1,3 %
Informacion Critica Expuesta	1,0 %
Contenido Abusivo - Spam	0,5 %
Contenido Abusivo - Pederastia	0,3 %
Disponibilidad - Fallo Hardware	0,3 %
Total general	100 %

Fuente: Mindefensa. Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT. La Ciberseguridad y Ciberdefensa en Colombia y los esfuerzos interinstitucionales para afrontar las nuevas amenazas emergentes en el ciberespacio.

Para el año 2019, el grupo de respuesta menciona un panorama informático nacional e internacional, en donde predominan los ataques a sectores bancarios, acceso a información gubernamental y figuras políticas, así como el ingreso no autorizado a millones de cuentas de correo electrónico, en donde se exponen al público los datos confidenciales de sus miembros.

[23] Mindefensa. Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT. La Ciberseguridad y Ciberdefensa en Colombia y los esfuerzos interinstitucionales para afrontar las nuevas amenazas emergentes en el ciberespacio. [en linea]. [Consulta: abril 26 de 2020]. Disponible en: https://web.certicamara.com/files/eventos/CiberseguridadCiberdefensaColombia.pdf

Continuando con los procesos de gestión de seguridad informática, el grupo de respuesta a emergencias colombiano, para el año 2019 realizó la identificación y clasificación de la infraestructura critica del país, en donde se hace mención de 13 sectores públicos, clasificados en 5 niveles de riesgo; dentro de los cuales destacan el sector TIC y electricidad como nivel de riesgo muy alto, Transporte y seguridad y defensa con nivel alto, industria comercio y turismo con nivel medio, salud y educación con nivel de riesgo moderado y por ultimo agricultura y medio ambiente con riesgo bajo.[24]

5.2 ALCANCE Y FACTIBILIDAD DE UN CSIRT NACIONAL EN LA EMPRESA PLATINO SISTEMAS.

Actualmente platino sistemas cuenta con la infraestructura tecnológica necesaria para brindar servicios de seguridad para la protección de la Información a nivel nacional, por lo cual dentro de la visión de la organización esta crear un equipo de Respuesta a Incidentes Cibernéticos CSIRT el cual sea capaz de gestionar diferentes solicitudes y peticiones acerca de incidentes informáticos. Una vez analizado el panorama nacional en lo referente a la seguridad informática, se establecen diferentes puntos geográficos como referencia, así como los problemas informáticos de mayor incidencia en el país, los cuales son susceptibles de atención y gestión por parte de un CSIRT de carácter y ámbito nacional.

Debido a la extensión geográfica en la que se reportan los incidentes, un CSIRT deberá tener la capacidad de actuación nacional, así como las características que una organización de este ámbito requiere, entre ellos ser un punto de coordinación y comunicación con otros centros de respuesta y atender reportes de incidentes cibernéticos sin importar el ámbito.

Por lo anteriormente expuesto se perfila como factible la implementación de un CSIRT en la empresa platino sistemas el cual tenga un ámbito de actuación y alcance nacional para atender y gestionar reportes de incidentes que cubran los requerimientos colombianos.

[24] Ibid. clasificación estructura critica del país.

5.3 TIPIFICACIÓN DE DELITOS E INCIDENTES INFORMÁTICOS EN COLOMBIA

Este tipo de incidentes que se tiene directa relación con la ciberseguridad se encuentran tipificados como los más comunes en Colombia y representan grandes cantidades de ocurrencia en el territorio.

5.3.1 *Skimming*- fraude con tarjetas débito y crédito. A través de esta técnica, los delincuentes realizan un clonado del dispositivo físico utilizado por la victima a la hora de pasarlo a través de una banda magnética, la cual, se encuentra ubicada en su mayoría de veces, en los cajeros automáticos de lugares como gasolineras, restaurantes, supermercados y en cualquier otro donde se disponga de pagos a través de dinero electrónico.
Guerrero J[25] realiza las siguientes recomendaciones para evitar ser víctima de este delito:

- Asegurarse que el teclado del cajero automático este en buenas condiciones para la transacción.
- Notificar al banco en caso de que la ranura de la tarjeta presente anomalías.
- Evite usar el cajero automático si existen cámaras de video que capturen su clave.
- No acepte ningún tipo de ayuda de extraños.
- Hacer uso de tarjetas con chip inteligente. Estas aún no han podido ser clonadas.

5.3.2 *Phishing*. Es un método de ataque informático en la categoría de suplantación de identidad, en la cual el atacante, se hace pasar por una persona o identidad legitima, este a través del uso de ingeniería social, trata de capturar datos o credenciales del acceso a la víctima. Esta modalidad de ataque puede verse a través del uso de correos electrónicos (modalidad más común) o en llamadas telefónicas.

[25] GUERRERO, J. Incidentes informáticos en Colombia en los últimos 10 años. [Internet]. 2018. [citado: 2020, abril] Disponible en: https://repository.unad.edu.co/handle/10596/31941

Existe una gran variedad de técnicas utilizadas para este tipo de ataque, entre ellas envió de correos electrónicos masivos, modificación de páginas web para simular un aspecto similar, así como modificaciones de la URL de las páginas web legitimas.

Un ejemplo sencillo de ataque de phishing es el envío de correos electrónicos a los miembros de una organización, en donde se ínsita a abrir enlaces o URL's contenidas en el cuerpo del mensaje, a través de frases sugestivas o que llamen la atención de la víctima. Al abrir este enlace se remitirá a esta a una dirección web que podría robar diferente tipo de información.

Aunque reconocer una página web o un correo electrónico ilegitimo, en muchas ocasiones no es nada fácil, se deberán seguir diferentes recomendaciones para evitar ataques de *phishing*, sitios Web como *InfoSpyware*[26] proporciona algunas como:

- No entregar datos por correo electrónico.
- No dar clic a enlaces de los cuales dude su procedencia
- Verifique la información recibida con la entidad que se está comunicando a través del correo electrónico.
- Si detecta un correo fraudulento, ignórelo
- Comprobar el modo seguro de las páginas web a través del navegador (https)

El *phishing* es una de las modalidades de ataque informático más popular en Colombia, ya que como lo registra el diario la república en un artículo del año 2019, mediante un informe dado a través de "*Sophos*", firma especializada en seguridad de redes y *endpoint*, se detalla:

> El 53 % de que fueron blanco de un ataque cibernético manifestaron que fue por un correo electrónico en el que el delincuente se hace pasar por una empresa o institución de confianza para obtener información confidencial de su víctima como contraseñas o números de tarjetas de crédito[27].

[26] InfoSpyware. ¿Qué es el Phishing? [en línea]. [Consulta abril 23 de 2020]. Disponible en: https://www.infospyware.com/articulos/que-es-el-phishing/

[27] Diario La República Colombia fue uno de los países con más ataques cibernéticos el año pasado. (Julio 2019). [en línea]. [Consulta: abril 23 de 2020]. Disponible en: ttps://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

De esta manera los empresarios encuestados por “Sophos” mencionaron que en promedio transcurren alrededor de 13 horas para detectar la amenaza, tiempo en el cual el atacante puede hacer y deshacer.

Dentro de los casos más populares de *phishing* en Colombia se encuentran:

- Carta Nigeriana o fraude 419 (intento de *phishing* a través de correo electrónico)
- Intento de estafa a través de correo electrónico suplantando a Bancolombia, entidad bancaria más grande del país.
- Fraude banco Falabella

5.3.3 *Vishing*. El termino *vishing* es una combinación de los términos “*Voice*” y “*Phishing*”, con lo cual la víctima es contactada a través de llamadas telefónicas y por medio de técnicas como ingeniería social, tratan de convencer a la víctima para que entregue información personal o datos sensibles que pueden ser utilizados para estafarlos.

Para evitar estos ataques se deberán seguir las mismas medidas o recomendaciones para el *phishing*, con lo cual no se deberá entregar información a través de llamadas telefónicas o responder a mensajes de texto donde se solicite datos confidenciales.

5.3.4 *Malware*. Como lo define AVG, antivirus propiedad del grupo checo, AVG Technologies, a través de su web oficial, el termino *malware* es una contracción de *malicious software*, con lo cual se definiría como un programa informático creado con fines maliciosos, este tiene como fin dañar dispositivos, robar información, afectar sistemas de información, entre otros.
De igual manera AVG realiza una calificación de *software* malicioso en los siguientes tipos.

- Virus: estos tienen la capacidad de integrarse con los demás programas del sistema, con lo cual puede propagarse sin control en el sistema, con lo cual podría eliminar, alterar e inutilizar alguna información. Los virus tienen la apariencia de archivos ejecutables con la extensión “.exe”.

- Troyanos: tienen como objetivo hacerse pasar por un *software* legitimo con la finalidad de abrir puertas traseras o permitir a los intrusos tomar el control del sistema donde resida.

- *Spyware*: como su nombre lo indica este *software* malicioso espía a sus víctimas, con lo cual realiza un registro de sus actividades en el equipo local y a través de internet, en donde almacena credenciales de acceso y demás información importante de la víctima.

- Gusanos: la finalidad de los gusanos es propagarse a través de la red o de los archivos del equipo infectado, con el fin de consumir recursos y afectar el rendimiento del sistema.

- *Ransomware*: *Malware* famoso recientemente. Este encripta y bloquea los datos de un computador, con el fin de solicitar un pago por parte del atacante para liberar nuevamente la computadora.

- *Adware*: *malware* de carácter publicitario, el cual, aunque no sea de carácter malicioso puede ser una molestia para la victima si la cantidad de publicidad es muy grande.

- *Botnets*: Son redes de equipos infectados forzados a trabajar en colaboración bajo el mandato de un atacante.

AVG realiza una serie de recomendaciones para evitar el *malware*, las cuales van desde la utilización de un antivirus, el cual puede ser instalado en la computadora personal de quienes hacen uso de internet, hasta seguir buenos hábitos de uso de redes como:

- Evitar ingresar a páginas web que generen desconfianza o totalmente desconocidas.

- Analizar los archivos descargados.

- Evitar hacer clic en enlaces enviados a través de correo electrónico

5.3.5 *Spoofing* El equipo de Oracle a través de su web oficial define al *spoofing* como:

> El *spoofing* consiste en usurpar una identidad electrónica para ocultar la propia identidad y así cometer delitos en Internet. Existen 3 tipos: *spoofing* de correo electrónico, *spoofing* de IP y *smart-spoofing* IP[28].

Por lo anterior, se puede entender al *spoofing*, como la técnica con la cual los atacantes suplantan sistemas informáticos, sean equipos físicos, correos electrónicos o direcciones web con el fin de hacerse parecer a entidades legitimas e interceptar o robar información de carácter confidencial.

En algunos casos específicos el *spoofing* a través de técnicas como de envenenamiento de ARP, permiten realizar suplantaciones de direcciones MAC entre dos equipos, funcionando de esta manera como un intermediario, con lo cual la comunicación entre estos dos será “escuchada”, sin que los involucrados tengan conocimiento alguno. De esta manera no se suplantarán correos o páginas web con la cual la victima interactúa directamente, solo habrá un sistema intervenido.

Guerrero J[29], menciona los siguientes tipos de suplantación:

Suplantación de IP: técnica en la cual el atacante realiza una suplantación a la dirección IP de un *host* o servidor.

Suplantación de ARP: el envenenamiento o suplantación de ARP, consiste en asociar la dirección MAC de un equipo en la comunicación de dos máquinas en una red, con el fin de estar a la escucha de los datos que transiten entre la comunicación establecida.

Suplantación de DNS: técnica que falsea la relación entre el dominio y la dirección IP asociada. Con este método se pueden obtener, la IP o nombre del DNS.

Suplantación de correo electrónico: a través de esta técnica, se suplantan direcciones de correo electrónico, con lo cual la victima recibe e ingresa información solicitada con el fin de robar datos confidenciales.

[28] Oracle. ¿Qué es el Spoofing? [en línea]. [Consulta: abril 27 de 2020]. Disponible en: https://www.oracle.com/es/database/security/que-es-el-spoofing.html
[29] Opt. Cit. P. 72

5.3.6 *Criptojacking*. Panda Security[30] define el *criptojacking* o minería de criptomonedas maliciosa como la vulneración de un dispositivo electrónico como PC, Smartphone o diferentes equipos en red para realizar procesos de extracción de monedas digitales. De esta manera no se accede a los equipos, solamente se realiza el minado de criptomonedas secuestrando los recursos informáticos de otros usuarios.

Este acceso no autorizado a los recursos de diferentes equipos se produce gracias a la intromisión de personal con avanzados conocimientos en sistemas, los cuales logran tomar gran parte de los recursos de estos para realizar procesos de minado de criptomonedas, proceso que debido a la gran cantidad de cálculos matemáticos requieren de mucho procesamiento.

Un equipo o dispositivo puede resultar infectado debido al ingreso de sitios web dudosos o a través de la instalación sin consentimiento de algún *malware*.

Riesgos asociados al *Criptojacking*

El mayor riesgo asociado es el uso de recursos de sistemas de cómputo personales, aunque se pueden evidenciar diferentes problemas técnicos a nivel empresarial, como aumentos de facturas eléctricas, aminoramiento de rendimiento en equipos críticos, debido al uso excesivo de los mismos. Aunque el principal objetivo de este ataque es manipular los recursos de los dispositivos, el haber tomado el control de estos hace suponer un gran problema de seguridad que puede ser aprovechado por terceros.

5.4 CATÁLOGO DE SERVICIOS DEL CSIRT PLATINO SISTEMAS

Platino sistemas, al igual que cualquier equipo de respuesta ante incidentes informáticos, cuenta con la capacidad de ofrecer diferentes servicios de acuerdo con la categorización de sus usuarios, así como el personal técnico y profesional competente, por lo cual a continuación se listarán los tipos de servicios a ofrecer

[30] Panda Security. Criptojacking. [en linea]. [Consulta: abril 27 de 2020]. Disponible en: https://www.pandasecurity.com/es/security-info/cryptojacking/

Servicios Reactivos

Tratamiento de incidentes

- Recepción, diagnóstico y respuesta ante incidentes reportados por parte del área de comunicación del CSIRT.
- Reparaciones del área de sistemas.

Análisis de incidentes.

- Examen de la información entregada acerca del incidente reportado.
- Definición del alcance del incidente.
- Definición de las estrategias a implementar como solución al incidente.

Apoyo a la respuesta a incidentes

- Servicio de ayuda y orientación a través de líneas telefónicas, correo electrónico o asistentes remotos a las víctimas del incidente reportado.

Tratamiento de la Vulnerabilidad.

- Recopilación de la información acerca de las vulnerabilidades a nivel de *hardware* y *software* en medio del análisis de la vulnerabilidad reportada.

Análisis de la vulnerabilidad

- Servicios prestados al *hardware* y *software* en busca de aspectos vulnerables dentro del sistema.

Servicios Proactivos

Comunicados

- Comunicados a los clientes del CSIRT acerca de los procesos de desarrollo del equipo.
- Servicio de alertas de intrusos o de advertencia acerca de la detección de vulnerabilidades.

Evaluaciones y auditorias de seguridad

- Prestación de servicios de estudios, análisis, verificación y auditoría a la infraestructura de una organización, de acuerdo con la normatividad vigente.
- Prestación de servicios de detección de intrusos
- Procesos de revisión a los sistemas de detección existentes para definir políticas de atención a eventos que superen umbrales definidos como amenaza.

Servicios Complementarios

Análisis de riesgos y continuidad del negocio.

- Proceso de evaluación cualitativa y cuantitativa de los riesgos activos en una organización.

Servicios de consultoría en seguridad informática

- Asesoría para mejores prácticas a implementar dentro de la organización.
- Servicios de apoyo para la adquisición de infraestructura tecnológica de una empresa.

Concientización ante la problemática de seguridad

- Labores de gestión diarias para fomentar actividades cibernéticas más seguras.

Educación, formación y capacitación en temas de seguridad

- Servicio de entrega como herramientas de capacitación; en donde a través de folletos, seminarios, conferencias, cursos y tutoriales se capacitarán a individuos u organizaciones para implementar acciones seguras dentro de los procesos informáticos que se lleven.

5.5 CARACTERIZACIÓN Y MANUAL DE FUNCIONES DE LOS PERFILES DEL EQUIPO DE TRABAJO CSIRT.

Una vez se establecen los servicios a prestar por parte del CSIRT, es importante establecer el personal directivo, técnico y profesional que conforme el equipo de trabajo de la organización el cual ejecute las tareas y actividades necesarias para dar cumplimiento a los objetivos trazados para el equipo.

Como lo menciona la Agencia Europea de Seguridad de las Redes y de la Información, ENISA en su guía de creación de un CSIRT[31], no es fácil mencionar con exactitud la cantidad de personal técnico y profesional necesario para conformar el CSIRT, ya que todo dependerá de la cantidad de servicios ofrecidos y el ambiente de desarrollo del equipo.

Autores como Van der Heide[32] presentan algunos valores cuantitativos aproximados para las cantidades de recurso humano en un CSIRT, en donde se menciona:

- 4 trabajadores a tiempo completo para atender 2 tipos de servicios de respuesta a incidentes.
- 6-8 trabajadores a tiempo completo para CSIRT en horarios de atención de oficina.
- 12 o más trabajadores para un CSIRT con horarios de atención 24X7.

Por lo anterior se crea el manual de funcionas para el equipo de respuesta ante incidentes informáticos CSIRT para la empresa PLATINO SISTEMAS, el cual se dispone en el índice presentado en la tabla 2.

[31] ENISA. Op. Cit., p.26
[32] VAN DER HEIDE, M. (2017). Establishing a CSIRT. Thailand: Thailand Computer Emergency Response Team.

Tabla 2. índice del manual de funciones y competencias laborales.

	CÓDIGO	No. CARGOS
NIVEL DIRECTIVO		
Director General	01	1
Director de Operaciones	02	1
Director de Tecnologías e Información	03	1
NIVEL PROFESIONAL		
Capacitación y apoyo externo	010	1
Marketing y comunicaciones	011	1
Apoyo Jurídico	012	1
NIVEL TÉCNICO		
Técnico administrativo en gestión de redes	020	3
Técnico administrativo en gestión de equipos y sistemas informáticos.	021	3
TOTAL		12

Fuente: Propia del autor

En la tabla 2, se observa que para el CSIRT Platino sistemas, se ha sugerido la creación de 3 niveles laborales, los cuales tendrán diferentes responsabilidades dentro de la organización y estructura jerárquica del CSIRT. Se hace importante que para cada uno de estos se mencione su propósito general, la descripción de las funciones a realizar, el nivel de conocimiento básico del personal a ocupar el cargo creado, así como los requisito de estudio y experiencia para desarrollar la labor, lo cual será mencionado en el siguiente apartado.

5.5.1 Nivel Directivo. El cual tendrá a cargo funciones de dirección, manejo de personal dentro de dependencias y toma de decisiones dentro de los procesos del equipo de respuesta.

I.IDENTIFICACIÓN

NIVEL	DIRECTIVO
DENOMINACION DEL EMPLEO	Director General
CÓDIGO	001
NUMERO DE CARGOS	UNO (1)
DEPENDENCIA	Dirección
CARGO DEL JEFE INMEDIATO	N.A.

II. PROPOSITO PRINCIPAL

Establecer las líneas de la organización y llevar a cabo la planificación estratégica, así como establecer acuerdos de cooperación con otras organizaciones CSIRT.

III. DESCRIPCION DE FUNCIONES

1. Obtener las aprobaciones necesarias para el funcionamiento del CSIRT.
2. Realizar labores de dirección estratégica.
3. Supervisar las de actividades del CSIRT.
4. Realizar procesos de vinculación externa e interna de la organización
5. Realizar procesos de gestión presupuestal.
6. Establecer comunicación con el público/medios del ambiente donde se desarrolla el CSIRT.
7. Realizar procesos de contratación de Recursos humanos y tecnológicos.
8. Adquirir e implementar infraestructura tecnológica.
9. Definir planes de comunicación y dispersión de información.
10. Definir políticas de procedimientos y procedimientos del CSIRT.
11. Ejecutar los planes de acción para el CSIRT.

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Teoría general de sistemas.
2. Estrategias de desarrollo organizacional.
3. Seguridad informática
4. Administración de organizaciones.
5. Normatividad en seguridad informativa

6. Normas y estándares de seguridad informática.
7. Dirección de personal y recursos humanos.

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ÁREA DEL CONOCIMIENTO	
INGENIERÍA, ADMINISTRACION EMPRESARIAL	
NUCLEO BÁSICO DE CONOCIMIENTO	
Ingeniería de sistemas y afines	
Administración y afines	
ESTUDIO	**EXPERIENCIA**
Título profesional en cualquier núcleo básico del conocimiento.	Mas de 10 años de experiencia profesional relacionada
ALTERNATIVAS	
ESTUDIO	**EXPERIENCIA**
Título de posgrado en áreas de seguridad informática (especialización maestría, Doctorado), y/o áreas afines a administración y manejo empresarial.	Título de posgrado en la modalidad de especialización en áreas relacionadas con las funciones del cargo.
Certificaciones en seguridad informática con entidades de carácter internacional (ISACA, CISSP, CISM, CISA o similares).	N/A

I.IDENTIFICACIÓN

NIVEL	DIRECTIVO
DENOMINACION DEL EMPLEO	Director de Operaciones
CÓDIGO	002
NUMERO DE CARGOS	UNO (1)
DEPENDENCIA	Dirección de operaciones
CARGO DEL JEFE INMEDIATO	Director General.

II. PROPOSITO PRINCIPAL

Realizar labores de gestión, monitoreo y el análisis de incidentes informáticos, que sean reportados al CSIRT.

III. DESCRIPCION DE FUNCIONES

1. Liderar procesos diarios del CSIRT.
2. Analizar, monitorear y registrar los incidentes informáticos reportados al CSIRT.
3. Coordinar acciones de respuesta ante incidentes informáticos.
4. Tratamiento de incidentes
5. Gestionar procesos de recepción, diagnóstico y respuesta ante incidentes reportados por parte del área de comunicación del CSIRT.
6. Definir el alcance de los incidentes reportados ante el CSIRT
7. Gestionar las estrategias a implementar como solución a incidentes informáticos.
8. Gestionar las labores de recopilación de la información acerca de las vulnerabilidades reportadas.
9. Realizar y gestionar procesos de estudios, análisis, verificación y auditoría a la infraestructura de acuerdo con las normatividades vigentes.

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Teoría general de sistemas
2. Normatividad en seguridad informática
3. Manejo de incidentes informáticos
4. Modelos y estándares de seguridad informática.
5. Manejo de reportes.
6. Informática Forense
7. Aseguramiento de la información

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ÁREA DEL CONOCIMIENTO	
INGENIERÍA, ADMINISTRACION EMPRESARIAL	
NUCLEO BÁSICO DE CONOCIMIENTO	
Ingeniería de sistemas y afines	
ESTUDIO	**EXPERIENCIA**
Título profesional en cualquier núcleo básico del conocimiento.	Mas de 10 años de experiencia profesional relacionada
Título de posgrado en áreas de seguridad informática (especialización maestría,	Título de posgrado en la modalidad de especialización en áreas relacionadas con las funciones del cargo.

Doctorado), y/o áreas afines a administración y manejo empresarial.	
Certificaciones en seguridad informática con entidades de carácter internacional (ISACA, CISSP, CISM, CISA o similares).	N/A

I.IDENTIFICACIÓN

NIVEL	DIRECTIVO
DENOMINACION DEL EMPLEO	Director de Tecnologías de Información.
CÓDIGO	003
NUMERO DE CARGOS	UNO (1)
DEPENDENCIA	Dirección de TI
CARGO DEL JEFE INMEDIATO	Director General.

II. PROPOSITO PRINCIPAL

Implementar y administrar todos los sistemas que controlan y maneja el CSIRT tales como: correo electrónico, página web, servidor de archivos, el sistema de gestión de "*tickets*", la supervisión del sistema, la red y los servidores de seguridad del CSIRT.

III. DESCRIPCION DE FUNCIONES

1. Gestionar las labores de administración de la infraestructura disponible por el CSIRT para la labor diaria.
2. Gestionar tareas de monitoreo de los equipos informáticos activos del CSIRT.
3. Gestionar y mantener la infraestructura de la red CSIRT.
4. Gestionar el apoyo en la ayuda a respuestas de incidentes informáticos en casos relacionados a la red.
5. Gestionar la asistencia técnica ante respuestas a incidentes cuando se necesite conocimientos en sistemas de TI.
6. Gestionar la prestación de servicios al hardware y software en busca de aspectos vulnerables dentro de un sistema informático.

7. Gestionar la prestación de servicios de detección de intrusos cuando sea requerido.
8. Gestionar el servicio de alertas de intrusos o de advertencia acerca de la detección de vulnerabilidades cuando sea requerido.

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Seguridad en redes de computación.
2. Manejo de bases de datos.
3. Normatividad en seguridad informática
4. Manejo de incidentes informáticos
5. Modelos y estándares de seguridad informática.
6. Arquitectura de computadores
7. Manejo de reportes.
8. Montaje y mantenimiento en equipos de cómputo.

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ÁREA DEL CONOCIMIENTO	
INGENIERÍA, ADMINISTRACION EMPRESARIAL	
NUCLEO BÁSICO DE CONOCIMIENTO	
Ingeniería de sistemas y afines	
ESTUDIO	**EXPERIENCIA**
Título profesional en cualquier núcleo básico del conocimiento.	Mas de 10 años de experiencia profesional relacionada
Título de posgrado en áreas de seguridad informática (especialización maestría, Doctorado), y/o áreas afines a administración y manejo empresarial.	Título de posgrado en la modalidad de especialización en áreas relacionadas con las funciones del cargo.
Certificaciones en seguridad informática con entidades de carácter internacional (ISACA, CISSP, CISM, CISA o similares).	N/A

5.5.2 Nivel Profesional. Este nivel proporcionará el apoyo profesional al equipo de respuesta en aspectos en que se requiera lograr comunicación entre dependencias u otros CSIRT, así como apoyos jurídicos y legales en los que la organización crea conveniente.

I.IDENTIFICACIÓN

NIVEL	Profesional
DENOMINACION DEL EMPLEO	Capacitación y apoyo externo
CÓDIGO	010
NUMERO DE CARGOS	UNO (1)
DEPENDENCIA	Dirección de operaciones
CARGO DEL JEFE INMEDIATO	Director General.

II. PROPOSITO PRINCIPAL

Ofrecer capacitaciones de actualización en temas de manejos de incidentes informáticos y temas de seguridad informática, además se ofrecer servicios de consultoría externa cuando el CSIRT lo solicite.

III. DESCRIPCION DE FUNCIONES

1. Impartir capacitaciones a través de medios presenciales y virtuales en temas referentes a seguridad informática dentro del equipo CSIRT y en servicios de consultoría externa para diferentes organizaciones.

2. Prestar asesoría en análisis de riesgos y continuidad del negocio.

3. Prestar servicios de consultoría en seguridad informática

4. Prestar servicios de asesoría para mejores prácticas a implementar dentro de la organización.

5. Servicios de apoyo para la adquisición de infraestructura tecnológica de una empresa.

6. Labores de gestión diarias para fomentar actividades cibernéticas más seguras.

7. Educación, formación y capacitación en temas de seguridad

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Normatividad en seguridad informática
2. Manejo de incidentes informáticos
3. Modelos y estándares de seguridad informática.
4. Manejo de reportes.
5. Pedagogía y acompañamiento tutorial.

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ÁREA DEL CONOCIMIENTO	
INGENIERÍA, ADMINISTRACION EMPRESARIAL	
NUCLEO BÁSICO DE CONOCIMIENTO	
Ingeniería de sistemas y afines	
ESTUDIO	**EXPERIENCIA**
Título de posgrado en áreas de seguridad informática (especialización maestría, Doctorado), y/o áreas afines a administración y manejo empresarial.	Título de posgrado en la modalidad de especialización en áreas relacionadas con las funciones del cargo.
Certificaciones en seguridad informática con entidades de carácter internacional (ISACA, CISSP, CISM, CISA o similares).	N/A

I.IDENTIFICACIÓN

NIVEL	Profesional
DENOMINACION DEL EMPLEO	Marketing y Comunicaciones
CÓDIGO	011
NUMERO DE CARGOS	UNO (1)
DEPENDENCIA	Dirección de operaciones
CARGO DEL JEFE INMEDIATO	Director General.

II. PROPOSITO PRINCIPAL

Ofrecer servicios de comunicación dentro y fuera del CSIRT. Ser el representante o vocero del equipo ante diferentes eventos y ser el canal de comunicación y mercadeo del equipo de respuesta ante incidentes informáticos.

III. DESCRIPCION DE FUNCIONES

1. Elaborar material publicitario (físico y/o digital) para promocionar los servicios del CSIRT.
2. Establecer canales de comulación entre las dependencias y recurso humano del CSIRT
3. Asistir a eventos de diferente índole como representante y vocero del CSIRT.
4. Elaborar planes de mercado publicitario para el CSIRT.
5. Comunicados a los clientes del CSIRT acerca de los procesos de desarrollo del equipo.
6. Servicio de alertas de intrusos o de advertencia acerca de la detección de vulnerabilidades a los miembros del CSIRT.
7. Prestación del servicio de entrega como herramientas de capacitación; en donde a través de folletos, seminarios, conferencias, cursos y tutoriales se capacitarán a individuos u organizaciones para implementar acciones seguras dentro de los procesos informáticos que se lleven.

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Manejo de relaciones personales
2. Manejo de medios audiovisuales
3. Locución
4. Presentación de informes
5. Medios publicitarios
6. Marketing digital

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ÁREA DEL CONOCIMIENTO
INGENIERÍA, ADMINISTRACION EMPRESARIAL
NUCLEO BÁSICO DE CONOCIMIENTO
Comunicación social y afines
Marketing

ESTUDIO	EXPERIENCIA
Título Profesional en áreas de comunicación social y/o marketing digital	Mas de 3 años de experiencia profesional relacionada

I.IDENTIFICACIÓN

NIVEL	Profesional
DENOMINACION DEL EMPLEO	Apoyo Jurídico
CÓDIGO	012
NUMERO DE CARGOS	UNO (1)
DEPENDENCIA	Dirección
CARGO DEL JEFE INMEDIATO	Director General.

II. PROPOSITO PRINCIPAL

Brindar apoyo y asesoría jurídica en los casos en que el CSIRT lo requiera ante la presencia o reporte de un incidente informático que involucre acciones legales de acuerdo con la normatividad vigente.

III. DESCRIPCION DE FUNCIONES

1. Redacción de cláusulas contractuales o políticas internas.
2. Coordinar una investigación interna del incidente reportado.
3. Elaborar y presentar la denuncia correspondiente cuando se requiera.
4. Preparar los procedimientos judiciales pertinentes.
5. Actuar como interlocutor con las fuerzas y cuerpos de seguridad.
6. Gestionar junto con el área de comunicación de la empresa la información a transmitir sobre el incidente informático presentado.
7. Proteger la responsabilidad de directivos y administradores
8. Gestionar la crisis de reputación de la empresa.

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Normatividad vigente en el campo de desempeño
2. Manejo de medios de comunicación.
3. Código penal
4. Aspectos éticos y legales de ciberseguridad.

5. Ley 1273 de 2009
6. CONPES 3709

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ÁREA DEL CONOCIMIENTO	
INGENIERÍA, ADMINISTRACION EMPRESARIAL	
NUCLEO BÁSICO DE CONOCIMIENTO	
Derecho y afines	
ESTUDIO	**EXPERIENCIA**
Título profesional en el núcleo básico del conocimiento. Tarjeta Profesional en los casos requeridos según normatividad legal vigente Título de posgrado en Derecho de las nuevas tecnologías o Derecho Digital.	Mas de 3 años de experiencia profesional relacionada

5.5.3 Nivel Técnico. A través de este nivel se identificará el personal de apoyo que estará bajo cargo de los niveles directivos y que realizarán las funciones que desde este nivel se disponga dentro del equipo de respuesta.

I.IDENTIFICACIÓN

NIVEL	Técnico - tecnológico
DENOMINACION DEL EMPLEO	Técnico administrativo en gestión de redes
CÓDIGO	020
NUMERO DE CARGOS	TRES (3)
DEPENDENCIA	Dirección de TI
CARGO DEL JEFE INMEDIATO	Director de tecnologías e información.

II. PROPOSITO PRINCIPAL

Administrar los sistemas que controlan y maneja el CSIRT tales como: correo electrónico, página web, servidor de archivos, el sistema de gestión de “tickets” y demás actividades asignadas por el jefe inmediato inherentes al cargo o dependencia.

III. DESCRIPCION DE FUNCIONES

1. Realizar las labores de administración de la infraestructura disponible por el CSIRT para la labor diaria.
2. Realizar tareas de monitoreo de los equipos informáticos activos del CSIRT.
3. Realizar procesos y actividades de mantenimiento a la infraestructura de la red CSIRT.
4. Brindar apoyo en la ayuda a respuestas de incidentes informáticos en casos relacionados a la red.
5. Brindar asistencia técnica ante respuestas a incidentes cuando se necesite conocimientos en sistemas de TI.
6. Prestar servicios al *hardware* y *software* en busca de aspectos vulnerables dentro de un sistema informático.
7. Prestar servicios de detección de intrusos cuando sea requerido.
8. Atender a solicitudes virtuales o físicas en el área requerida en el reporte de incidentes informáticos del CSIRT.
9. Entregar reportes de los incidentes informáticos reportados en el CSIRT (atendidos y en espera).

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Seguridad en redes de computación.
2. Manejo de Normatividad básica en seguridad informática
3. Manejo de incidentes informáticos de 1 nivel.
4. Arquitectura de computadores
5. Manejo de reportes.
6. Montaje y mantenimiento en equipos de cómputo.

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ÁREA DEL CONOCIMIENTO	
INGENIERÍA, ADMINISTRACION EMPRESARIAL	
NUCLEO BÁSICO DE CONOCIMIENTO	
Ingeniería de sistemas y afines	
Técnico – tecnólogo en sistema de información	
ESTUDIO	**EXPERIENCIA**
Título profesional en cualquier núcleo básico del conocimiento.	Mas de 2 años de experiencia profesional relacionada

I.IDENTIFICACIÓN

NIVEL	Técnico - tecnológico
DENOMINACION DEL EMPLEO	Técnico administrativo en gestión de equipos y sistemas informáticos.
CÓDIGO	020
NUMERO DE CARGOS	TRES (3)
DEPENDENCIA	Dirección de Operaciones
CARGO DEL JEFE INMEDIATO	Director de Operaciones

II. PROPOSITO PRINCIPAL

Atención, análisis y monitoreo de los incidentes informáticos reportados a través de las diferentes vías de comunicación implementadas en el CSIRT y demás actividades asignadas por el jefe inmediato inherentes al cargo o dependencia.

III. DESCRIPCION DE FUNCIONES

1. Atender y resolver los procesos diarios del CSIRT.
2. Analizar, monitorear y registrar los incidentes informáticos reportados al CSIRT.
3. Coordinar junto con el jefe inmediato las acciones de respuesta ante incidentes informáticos.
4. Dar solución y tratamiento a los incidentes informáticos reportados al CSIRT
5. recibir, diagnosticar y dar respuesta a los incidentes reportados por parte del área de comunicación del CSIRT.
6. Definir junto con el equipo de respuesta, el alcance de los incidentes reportados ante el CSIRT
7. Realizar las labores de recopilación de la información acerca de las vulnerabilidades reportadas.
8. Realizar y gestionar procesos de estudios, análisis, verificación y auditoría a la infraestructura de acuerdo con las normatividades vigentes.
9. Entregar reportes de los incidentes informáticos reportados en el CSIRT (atendidos y en espera).

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Manejo de Normatividad básica en seguridad informática
2. Manejo de incidentes informáticos de 1 nivel
3. Manejo de reportes.
4. Inspección de hardware y software
5. Manejo de herramientas para el aseguramiento de la información

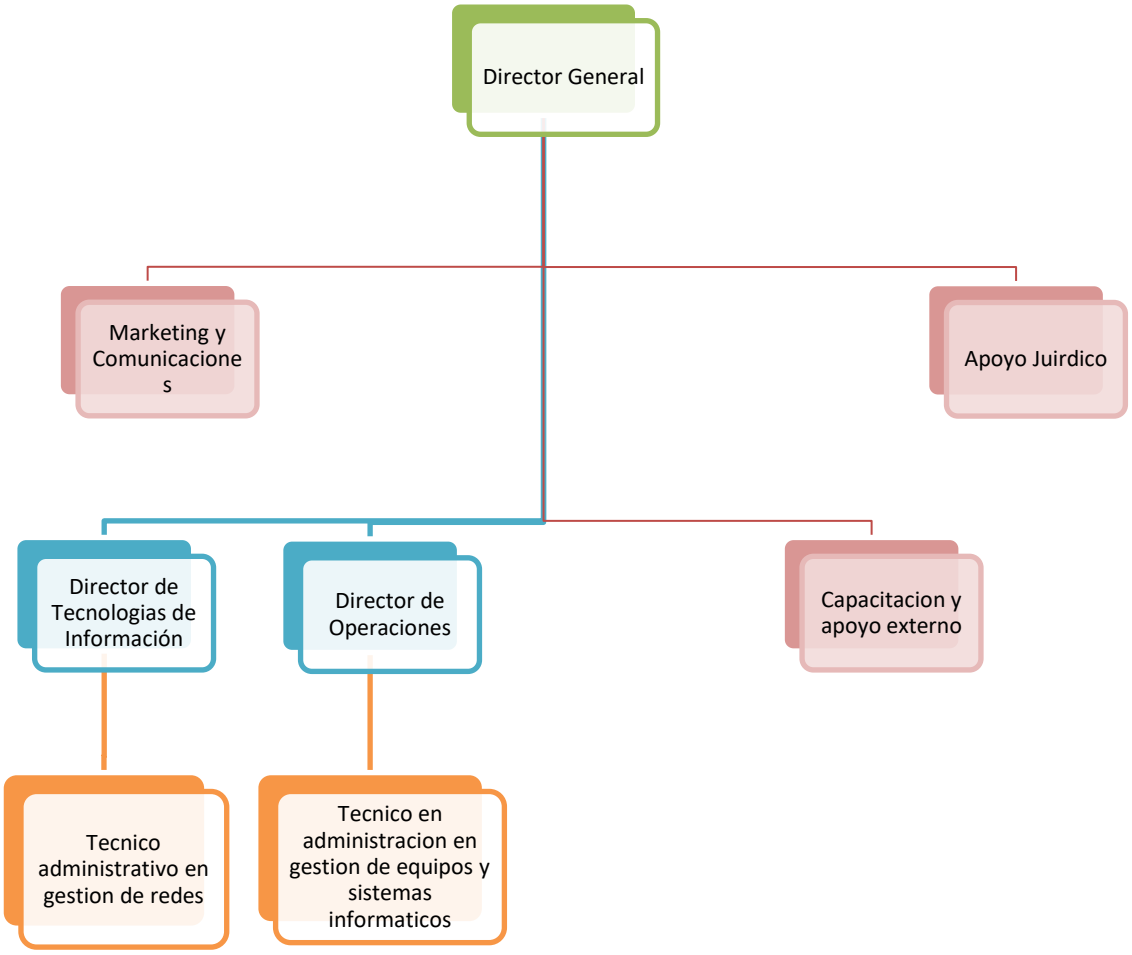
V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ÁREA DEL CONOCIMIENTO	
INGENIERÍA, ADMINISTRACION EMPRESARIAL	
NUCLEO BÁSICO DE CONOCIMIENTO	
Ingeniería de sistemas y afines	
Técnico – tecnólogo en sistema de información	
ESTUDIO	**EXPERIENCIA**
Título profesional en cualquier núcleo básico del conocimiento.	Mas de 2 años de experiencia profesional relacionada

5.6 Estructura Orgánica Sugerida CSIRT

Una vez se ha definido los perfiles profesionales y técnicos del CSIRT, se hace necesario presentar de forma clara la estructura orgánica del mismo. Para este tipo de casos, un diagrama jerárquico plasma de manera correcta las dependencias y cargos dentro de la estructura organizacional, lo cual para la empresa PLATINO SISTEMAS puede observase en la Figura 3.

Figura 3. Estructura Orgánica CSIRT PLATINO SISTEMAS



Fuente: Propia del autor

5.7 MANUAL DE POLÍTICAS Y PROCEDIMIENTOS OPERACIONALES, DE OBLIGATORIEDAD

Platino sistemas al igual que muchas otras organizaciones, incluye un manual de procedimientos que establecen las formas y procesos a llevar a cabo dentro de la organización para asegurar que existe calidad entre estos y que garantizan a sus clientes y usuarios la efectividad de su labor, por lo tanto, se definen las políticas mínimas para su operabilidad en el área de seguridad informática.

5.7.1 Clasificación de la Información. Política que abarca los temas de protección y acceso a niveles de información de acuerdo con lo definido dentro de una organización que maneja SGSI**.**

Objetivo

Establecer niveles apropiados de protección a los activos de información del equipo de respuesta CSIRT, de acuerdo con su importancia y criticidad.

Alcance

Todos los miembros activos del equipo de respuesta a incidentes informáticos CSIRT de la empresa platino Sistemas". Director General, director de TI, Director de Operaciones. Profesionales y técnicos de apoyo.

Declaración

La clasificación de la información se dará a partir de una recopilación previamente preparada, planificada y ejecutada de un inventario de activos de la organización, el cual genera un registro de activos que detallará claramente el responsable o propietario del activo, así como el formato en el cual existe, el cual podrá ser:

- Físico
- Electrónico

Este activo de información estará dado en los siguientes cuatro niveles.

Confidencial, Tendrá un acceso restringido a la Dirección General, documentos tales como: información contable y financiera del CSIRT, bases de datos de los

integrantes del equipo CSIRT, acceso al correo electrónico de gerencia y relaciones públicas del CSIRT,
Restringido: Tendrán acceso restringido a directores de Área de Ti y de Operaciones, documentos tales como: informes de operaciones de acuerdo con el nivel organizacional, acceso a bases de datos de clientes del CSIRT, informes de gestión a incidentes informáticos, información de divulgación y promoción CSIRT, evaluaciones de desempeño de los integrantes del equipo CSIR y a las áreas que pertenecen
Interno: Tendrá un acceso general por miembros autenticados del equipo CSIRT, documentos tales como: documentos de apoyo para la gestión de incidentes informáticos y de acuerdo con el área que el personal pertenece.

Público: Tendrá un Acceso general por cualquier miembro del equipo CSIRT o personal interesado en las labores del equipo, documentos tales como: Misión y visión de la organización, Historia y estructura organizacional, Portafolios de servicios, puntos de contacto, dirección y atención al cliente.

5.7.2 Protección de Datos. Política definida por las organizaciones para dar cumplimiento a la normatividad vigente para el uso de datos personales en términos nacionales e internacionales**.**

Objetivo

Dar cumplimiento a lo dispuesto en la ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013 y lo consignado en el artículo 15 de la Constitución Política Colombiana, referente al tratamiento y protección de datos personales.

Alcance

Política aplicable a todos los activos de información del equipo de respuesta CSIRT, tales como bases de datos, correos electrónicos, archivos físicos y digitales.

Declaración

El CSIRT implementara los siguientes mecanismos para la protección de datos de acuerdo con la siguiente clasificación:

Información pública
La divulgación de datos públicos será autorizada y solo podrá ser difundida por

medio de los canales y medios establecidos y por el área y profesional de apoyo de comunicación social del CSIRT. Esta comunicación estará reglamentada o definida en los procesos de manejo de la unidad.

Información clasificada

Los Datos definidos como clasificados solo podrán ser divulgados previa autorización del director General o el director de área designado por este. Para efectos de divulgación, se deberá realizar el procedimiento establecido para el caso, en donde se deberá notificar a quienes reciban la información clasificada, de la naturaleza de esta y las condiciones para el tratamiento de los datos recibidos.

Información confidencial

Se define la prohibición de la divulgación de información catalogada como confidencial por parte de algún miembro del CSIRT “platino Sistemas”.

Para efectos de utilización de algún tipo de información confidencial en algún proceso requerido y de carácter obligatorio, se deberá contar con el consentimiento del propietario de los datos o información, diligenciando un formato de autorización del uso de su información y la firma de un acuerdo de uso de datos personales o confidenciales.

Información de miembros del equipo CSIRT

Toda la información personal y de vinculación laboral del equipo CSIRT serán almacenados y bajo la custodia del director general del CSIRT, los cuales estarán dispuestos bajo la aceptación y firma de las políticas el CSIRT al momento de la vinculación laboral.

Ley estatutaria

El equipo CSIRT de platino sistemas se acogerá a lo dispuesto según la ley estatutaria de 1266 de 2008[33], por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

[33] Congreso de la Republica. LEY ESTATUTARIA 1266 DE 2008. [en línea]. [Consulta septiembre 26 de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

5.7.3 Retención de la Información. Las organizaciones requieren definir el tiempo en que pueden almacenar información dentro de sus instalaciones o bajo su poder, por lo cual se establecen los tiempos de retención de acuerdo con el tipo de información y al medio de almacenamiento

Objetivo

Definir los tiempos de retención, almacenamiento y disposición en que el CSIRT de “platino Sistemas”, mantendrá o resguardará registros e información de que disponga la organización.

Alcance

Política aplicable a todos los activos de información del equipo de respuesta CSIRT, tales como bases de datos, correos electrónicos, archivos físicos y digitales.

Declaración

Se establecen los tiempos de retención de acuerdo con la tabla 3

Tabla 3. Tiempos de retención de registros - información

Tipo Información - Registro	**Tiempo de retención**
Acuerdos, términos de uso o contratos	10 años a partir de su celebración.
Reportes, informes y/o fichas de registro de incidentes informáticos	20 años.
Material Publicitario o de promoción del CSIRT	10 años.
Informes de carácter administrativo y financiero	20 años.
Correos electrónicos	Indefinido. Se debe gestionar su almacenamiento prolongado.
Comunicados.	Indefinido. Se debe gestionar su almacenamiento prolongado.
Hojas de Vida	5 años
Datos o especificaciones técnicas de equipos activos del equipo CSIRT	A disposición y permanencia del equipo activo en el equipo.
Informes de auditoría	Indefinido. Se debe gestionar su almacenamiento prolongado.
Presupuestos y planeación estratégica	10 años.
Estados financieros	10 años
Comprobantes de pago o cuentas bancarias	10 años.
Información dispuesta a través de medios digitales o bases de datos de clientes o procesos misionales del CSIRT	Indefinido. Se debe gestionar su almacenamiento prolongado.

Fuente: Propia del autor

5.7.4 Destrucción de la Información. Política que define los métodos para la destrucción, borrado o desecho de información que maneja la organización. En esta política se establece claramente las técnicas a utilizar para llevar a cabo dicho proceso.

Objetivo

Definir los medios, técnicas y mecanismos para la destrucción de información como registros, dispositivos físicos y/o digitales, para garantizar que una vez se cumplan los tiempos de retención, sean destruidos o eliminados de manera segura.

Alcance

Política aplicable a todos los activos de información del equipo de respuesta CSIRT, tales como bases de datos, correos electrónicos, archivos físicos y digitales.

Declaración

Una vez se cumplen con los tiempos de retención de la información, se hace necesario implementar procesos que aseguren la eliminación o destrucción de manera segura, por lo cual se utilizarán métodos de borrado que garanticen que esta no sea recuperada.

Para destruir cualquier tipo de información (Física o digital) se atiende el proceso

1. Realizar solicitud a través de formato establecido por el equipo de respuesta.
2. El propietario o responsable del activo, evalúa y da aval al proceso.
3. Generar reporte del personal involucrado en el proceso d destrucción.

Para activos de información magnética o digitalizada se utilizarán métodos como: desmagnetización, destrucción a través de *software* especializado y sobre escritura.

Para activos de información física se utilizarán métodos como desintegración, pulverización o incineración; métodos para destruir por completo los medios de almacenamiento. En casos como la utilización de papel se empleará el método de trituración, asegurando que el tamaño del fragmento generado sea lo suficientemente pequeño para evitar la restauración del medio.

INCIBE, en su guía sobre borrado seguro de la información[34] ofrece una comparativa para los tipos de destrucción de información. Ver tabla 4.

Tabla 4. Métodos de borrado Seguro.

Soporte	Tipo	Destrucción física	Desmagnetización	Sobre escritura
Discos Duros	Magnético	SI	Si	Si
Discos Flexibles	Magnético	SI	Si	Si
Cintas Backup	Magnético	SI	Si	Si
CD	Óptico	SI	No	No
DVD	Óptico	SI	No	No
Pendrive	Electrónico	SI	No	SI
Discos Duros SSD	Electrónico	SI	No	SI

Fuente: INCIBE. guía sobre borrado seguro de la información. [en línea]. [Consulta: 3 octubre de 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

5.7.5 Divulgación de Información. A través de esta política se establecerán los medios de los cuales dispondrá la organización para emitir comunicados internos y externos, teniendo presente el tipo de información o clasificación realizada de acuerdo con las políticas definidas previamente.

Objetivo

Definir los medios y espacios en los cuales el CSIRT podrá compartir, distribuir o divulgar la información interna o externa de la organización.

Alcance

[34] INCIBE. guía sobre borrado seguro de la información. [en línea]. [Consulta: 3 octubre de 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

Política aplicable a todos los activos de información del equipo de respuesta CSIRT, tales como bases de datos, correos electrónicos, archivos físicos y digitales.

Declaración

Según la política de clasificación de la información del equipo de respuesta “platino sistemas”

Confidencial, tendrá un acceso restringido a la Dirección General

Restringido, tendrán acceso restringido a directores de Área de Ti y de Operaciones.

Interno, tendrá un acceso general por miembros autenticados del equipo CSIRT.

Público, tendrá un acceso general por cualquier miembro del equipo CSIRT o personal interesado en las labores del equipo.

La información de carácter confidencial e interna solo podrá ser divulgada dentro del equipo de respuesta y con la autorización del director general.
Si por algún motivo la información de carácter confidencial es requerida por entidades de control u organismos judiciales, tales como contraloría, procuraduría, defensoría del pueblo, tribunales, entre otros, se deberá registrar la petición a través de control físico o digital, en donde repose la información solicitada, el consecutivo, fecha de recepción y respuesta de la solicitud.

La información de carácter restringida, como información personal o sensible de clientes del CSIRT, solo podrá ser divulgada previa autorización del propietario de la información, a través de formato de autorización de tratamiento de información y firmado por el propietario.

La información de carácter publica y de carácter digital será divulgada a través de redes sociales y pagina web del equipo de respuesta informático y contendrán información de contacto, tales como números telefónicos, correos institucionales y demás que permitan comunicarse con la organización. La información de carácter físico, como folletos, tarjetas de representación, vallas publicitarias, contendrán la misma información disponible a través de los canales digitales.
La divulgación de la información de carácter público estará a cargo y bajo responsabilidad del profesional de apoyo en comunicación social.

5.7.6 Acceso a la información. A través de esta política la organización define los mecanismos con los cuales se podrá acceder a la información perteneciente o bajo custodia de la entidad, así como el alcance y usuarios involucrados.

Objetivo

Establecer los medios, mecanismos y formas de acceder a la información de acuerdo con controles de acceso y propietarios de la información, del personal del CSIRT, para contralar el quien, como y cuando se accede a la información.

Alcance

Política aplicable a todos los activos de información del equipo de respuesta CSIRT, tales como bases de datos, correos electrónicos, archivos físicos y digitales.

Declaración

Basados en el modelo de control de acceso sugerido por el instituto de seguridad de España INCIBE[35], Platino Sistemas establecerá dos niveles de dificultad para el tratamiento de información, Básico (1) o avanzado (2).

Nivel 1: Los recursos y el esfuerzo para el acceso de la información se realiza a través de metodologías sencillas.

Nivel 2: Los recursos y el esfuerzo para el acceso de la información se realiza a través de metodologías complejas.

El equipo de respuesta CSIRT trabajará bajo la implementación de:

[35] INCIBE. Control de Acceso, Política de seguridad para Pyme. [en línea]. [Consulta: 6 de octubre de 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf

Usuarios y grupos

A través de la definición de usuarios y la pertenencia a ciertos grupos de trabajo se concederán permisos para el acceso de la información concerniente, tales como áreas de TI, gestión y dirección u operacionales.

Asignación de permisos a usuarios

A través de esta acción se otorgarán los permisos de ejecución, lectura o escritura, copia o eliminación de información dentro del personal de la organización, en donde prevalecería el acceso a la información con los mínimos privilegios disponibles.

Gestión cuentas de usuario.

Se realizará la gestión de las cuentas de usuario a través del administrador responsable del área de dirección TI del CSIRT, el cual dará de alta y baja las cuentas de correo electrónico, usuario y tipo dentro de la red del CSIRT y asignará los permisos de usuarios de acuerdo con el área a la cual pertenece. De igual manera hará gestión y entrega de las claves de acceso a los usuarios, utilizado mecanismos que aseguren la confidencialidad de las credenciales.

Una vez se de alta un usuario, se eliminarán los permisos de acceso a cuentas de correo, equipos locales o aplicaciones de manejo del CSIRT. De la misma manera se le solicitara al usuario dado de alta, hacer entrega de cualquier activo de información otorgado para el desarrollo de sus labores.

Alcance de los controles de acceso a información

Los controles de acceso a la información serán definidos según su alcance como:

Procesos, para personal directivo
Tecnología, para personal técnico
Personas, para todo el personal

Tabla 5. Alcance de los controles de acceso a información

Nivel	Alcance	Tipo control
1	Procesos	Política de grupos y usuarios
1	Procesos	Asignación de permisos
1	Tecnología	Creación y eliminación de cuentas de usuario
2	Tecnología	Mecanismos de autenticación
1	Tecnología	Revisión de permisos
1	Tecnología	Revocación de permisos

Fuente: INCIBE. Guía sobre borrado seguro de la información. [en línea]. [Consulta: 3 octubre de 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

5.7.7 Uso Apropiado de los sistemas. Sin importar la clase de organización o el ámbito que se desempeñe, es importante establecer la forma en que el uso de sus sistemas informáticos y estructurales serán utilizados, por lo cual se establecen las policitas de uso de estos.

Objetivo

Definir las acciones necesarias para utilizar los activos físicos de la organización, asegurando el buen uso de los sistemas y recursos del CSIRT

Alcance

Política aplicable a todos los activos físicos del equipo de respuesta, incluidos los sistemas informativos, infraestructura de red y gestión de TI.

Declaración

Organización CSIRT

A través de la dirección general y la dirección de TI, se definen los activos de la organización, en donde se establece un inventario claro de los equipos informáticos y de infraestructura física del CSIRT.

Los recursos informáticos y de tecnología de TI disponibles a través del inventario de activos de CSIRT, solo podrán ser utilizados por los integrantes del CSIRT platino

sistemas. Para uso de personal externo o terceros, deberá existir una autorización por parte de la dirección de TI.

La información registrada o soportada a través de los activos físicos de la organización estará a cargo de la dirección de TI, asegurando la privacidad, confidencialidad e integridad de la información y en términos generales a la infraestructura tecnológica. Esta área de TI, asegurara el acceso únicamente a usuarios del CSIRT previa solicitud a la dirección.

Usuarios

El equipo entregado al usuario será de uso personal y únicamente para las labores encomendadas dentro de la organización.

Se prohíbe el uso de *hardware* o *software* ajeno al configurado y entregado por la organización.

Las credenciales de acceso para los equipos informáticos, será entregada únicamente al responsable del equipo y será de uso personal e intransferible. Se prohíbe su divulgación.

Los usuarios están en la obligación de reportar al director de área encargada, las posibles anomalías, vulnerabilidades, incidentes o uso incorrecto y que atente contra las políticas de la organización.

Se debe hacer responsable de dispositivos de E/S y unidades de almacenamiento externa, en pro de la integridad, confidencialidad y disponibilidad de la información, haciendo uso de antivirus informáticos y copias de respaldo periódicas.

Se debe hacer un uso adecuado y medido, de los canales de comunicación y atención del CSIRT, tales como internet, llamadas telefónicas y correspondencia, evitando el uso o actividades ajenas a las tareas misionales de la organización.

El uso del correo electrónico y la información allí contenida es de propiedad de la organización, por lo cual se deberá hacer un uso responsable y apropiado del envío y recepción de la información de carácter sensible.

Software

El software adquirido por la organización deberá contar con las licencias de usos adecuadas y será responsabilidad de la dirección de TI mantenerlas por el tiempo adecuado.

La dirección de TI deberá mantener un control y revisión periódica de las licencias de uso de los activos informáticos de la compañía, llevando un control sobre los equipos existentes y la vigencia de las licencias adquiridas.

Redes

Los equipos activos de red serán configurados y administrados únicamente bajo la autorización y coordinación de la dirección de TI

Sera responsabilidad de la dirección de TI, asegurar el correcto funcionamiento y servicios prestados a través de la red, tales como internet o intranet.

5.7.8 Definición de incidentes de seguridad y política de eventos. A través de estas policitas el equipo de respuesta tendrá claro dentro del desarrollo de sus procesos misionales, cuáles de los reportes hechos por sus usuarios califican dentro de los criterios de actuación del CSIRT.

Objetivo

Determinar los criterios de actuación del CSIRT para definir y clasificar los incidentes informáticos reportados.

Alcance

Política aplicable al personal del CSIRT para el manejo de eventos presentados en la organización.

Declaración

Platino sistemas tratara los eventos e incidentes de acuerdo con lo mencionado por la norma ISO 27001 la cual manifiesta que:

> Un incidente informático se define a una sola o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una elevada probabilidad significativa de comprometer las operaciones de negocio y amenazando la seguridad de la información[36].

[36] SGSI, Blog especializado en sistemas de gestión de seguridad informática. [en línea]. [Consulta: octubre 25 de 2020]. Disponible en: https://www.pmg-ssi.com/2015/10/clasificar-incidentes-norma-iso-27001/

La severidad de los incidentes se clasifica por

Alto Impacto, Afectación de los activos de información considerados de impacto catastrófico los cuales afectan de forma directa el carácter misional de una organización, tales como la afectación del nombre de esta, afectaciones legales y de producción.

Medio Impacto, aquellos incidentes que involucren a los activos de una organización que influyen en procesos de esta, pero que no afectan el carácter misional.

Bajo Impacto, incidentes que afectan a activos de información categorizados como de baja importancia y que no interviene en las labores de carácter misionales u objetivos de un proceso. Estos incidentes se deben monitorizar para evitar que cambie dentro de la escala de calificación.

Urgencia y atención de incidentes.

Se brindará atención a los incidentes de acuerdo con el nivel de urgencia e impacto que este genere de acuerdo con la matriz de urgencia y riesgo establecida a continuación.

Tabla 6. Urgencia y atención de incidentes.

Impacto / Urgencia	Alto	Medio	Bajo
Alto	1	2	3
Medio	2	3	4
Bajo	3	4	5

Fuente: Propia del Autor

Se clasifica el impacto como el daño que se causa en la organización.
Se clasifica urgencia como la velocidad con la que la que se necesita dar solución al incidente.

La matriz de relación permite establecer la prioridad de cada incidente y se obtienen los valores:

Los incidentes de valor 1 y 2 son críticos con una relación entre la urgencia y el impacto elevada.

Los incidentes de valores 3 tienen una relación de criticidad moderada.

Los incidentes de valor 4 y 5 son clasificados como de criticidad leve, los cuales se establecerán en la cola de atención por parte de platino sistemas.

Clasificación de incidentes

Acceso no autorizado – intrusión, tipo de incidente que involucra el accionar de un individuo, *software*, *script*, sistema o código malicioso que logra el acceso lógico o físico y sin previa autorización del propietario de un sistema, aplicación, información o un activo de información.

Alteración de recursos o activos, tipo de incidente que involucra un individuo, *software*, script, sistema o código malicioso con la intención de afectar la integridad de la información de un sistema o la integridad de un activo de una organización.

Usos inapropiados de activos, tipo de incidente que involucra a individuos que van en contra de las políticas de uso de activos de una organización.

Denegación de recursos, tipo de incidente que involucra un individuo, *software*, script, sistema o código malicioso que deniega el uso autorizado de un activo de información.

Incidente múltiple, tipo de incidente que involucra más de una categoría
De las mencionadas.

Sin categoría, tipo de incidente que no ha sido clasificado anteriormente, estos deben monitorizarse para ajustar las políticas de incidentes y su clasificación e incluir las que sean necesarias.

5.7.9 política de gestión de Incidentes. Gracias a la definición de estas políticas, el equipo de respuesta tendrá claros los procesos para la atención de un incidente informático reportado De igual manera se actuará de manera precisa para la gestión de este.

Objetivo

Definir el proceso para llevar a cabo la gestión de incidentes en el CSIRT, el tiempo de respuesta del incidente de acuerdo con su tipo, así como los procedimientos a aplicar.

Alcance

Política aplicable al personal del CSIRT para el manejo de eventos presentados en la organización.

Declaración

Tratamiento en 5 pasos de acuerdo con la norma IOS/IEC27001

1. Notificación

Se recibe la notificación del incidente reportado por alguna organización, por parte de un individuo perteneciente a la misma. Y se asigna un identificativo del reporte o *ticket*

2. clasificación

El área y personal encargados del CSIRT “platino Sistemas” que recibe a la notificación del incidente, deberá realizar el proceso de clasificación de este.

3. Tratamiento

Conociendo del grado de criticidad y la urgencia del incidente, se establece el tiempo de respuesta o solución.

4. Cerrar el incidente

Una vez se resuelve el incidente se realiza el proceso de registro del tratamiento y solución, de la misma manera se da por cerrado el *ticket* abierto en la notificación y se envía la información correspondiente a la organización que reportó el incidente.

5. Registro

Se debe realizar un reporte o registro del incidente reportado y del tratamiento dado, con el fin de llevar una bitácora de incidentes y ofrecer planes de mejora o adecuación de los planes de actuación del CSIRT. Estos registros tienen gran funcionalidad como referente para futuros tratamientos a incidentes similares.

Tiempos de respuesta ante incidentes informáticos

Platino sistemas manejara los tiempos de respuesta a incidentes reportados por organizaciones de acuerdo con lo sugerido por el MINTIC en su guía para la gestión de incidentes informáticos[37] en el cual se evalúa el nivel de prioridad de forma cuantitativa como se observa de acuerdo con las tablas 7, 8 y 9

Tabla 7. nivel de prioridad

Nivel de criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0,50	Sistemas que apoyan más de una dependencias o proceso de la entidad.
Alto	0,75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1,00	Sistemas Críticos.

Fuente: MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

Se deben tener en cuenta dos conceptos fundamentales para la evaluación del impacto

[37] MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [en línea]. [Consulta: octubre 14 de 2020]. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Impacto Actual, el cual depende de la cantidad de daño que provoca el incidente al ser detectado, y el Impacto Futuro el cual depende de la cantidad de daño que pueda causar si no es solucionado

De esta manera se podrá calcular el nivel de prioridad de acuerdo con la tabla 8.

Tabla 8. Niveles de Impacto

Nivel de Impacto	Valor	Definición
Inferior	0,10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0,50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información.
Superior	1,00	Impacto alto en uno o más componentes de más de un sistema de información.

Fuente: MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

El nivel de prioridad se calculará de acuerdo con la ecuación

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)

Tabla 9. nivel de prioridad incidente

Nivel de Prioridad	Valor
Inferior	00,00 – 02,49
Bajo	02,50 – 03,74
Medio	03,75 – 04,99
Alto	05,00 – 07,49
Superior	07,50 – 10,00

Fuente: MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

Una vez obtenido el nivel de prioridad del incidente reportado se establecen los tiempos de atención del incidente por parte del CSIRT, los cuales pueden visualizarse en la tabla 10.

Tabla 10. Tiempos de atención a incidentes

Nivel de Prioridad	Tiempo de respuesta
Inferior	3 horas
Bajo	1 hora
Medio	30 min
Alto	15 min
Superior	5 min

Fuente: MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

Procedimiento para la gestión de incidentes en 5 pasos

Notificación

Se recibe la notificación o alerta a través de los canales físicos o virtuales que disponga el equipo de comunicaciones del CSIRT, en donde el usuario reporta el incidente informático. Esta notificación puede ser recibida por parte de los miembros técnicos del área de TI o de operaciones en el cual se recibirá y solicitaran los siguientes datos de acuerdo con el formato de reportes establecidos en el CSIRT (anexo A).

Nombre de quien reporta incidente.
Cargo en la organización.
Oficina o dependencia.
Contacto telefónico
Correo electrónico de contacto.
Fecha de reporte
Hora de reporte.
Personal que atiene el reporte
Descripción del incidente.

Las notificaciones podrán ser recibidas vía correo electrónico, llamadas telefónicas o en atención al usuario según se disponga por el equipo de comunicaciones.

Clasificación

El área de Operaciones recibe la notificación y el formato de reporte de incidente y realizara la clasificación del incidente basado en la política de definición de incidentes de seguridad y política de eventos. Allí se asignará el área o personal técnico encargado de dar tratamiento de acuerdo con los resultados de calificación. De ser necesario se hará la gestión de tratarlo a través del área de TI o de Operaciones. Se diligenciará el formato de reporte (anexo A) Con la siguiente información

Área asignada al tratamiento.
Responsable.
Fecha de recepción
Hora de recepción

Tratamiento

El área asignada para dar solución o tratamiento al incidente realiza el análisis correspondiente, en donde tomará las medidas que considere pertinentes según sea el caso. De acuerdo con la clasificación del incidente se utilizarán las herramientas informáticas, métodos o metodología necesaria para solucionarlo.

Si el caso es tratado *in situ*, se deberá reportar lo siguiente:

Lugar de desplazamiento
Fecha de desplazamiento
Área encargada.
Profesional responsable.
Herramientas utilizadas.

Si el caso fue resuelto a través de canales virtuales se reportará lo siguiente:

Área encargada.
Profesional responsable.
Herramientas utilizadas.

Dentro del reporte de tratamiento se deberá mencionar el tipo y descripción de tratamiento dado al incidente para establecer el cierre del incidente.

Cerrar incidente.

Una vez se diligencie el reporte del tratamiento del incidente, se realiza la notificación al área de comunicaciones para que sea notificado de la solución a la organización que reporto el incidente.

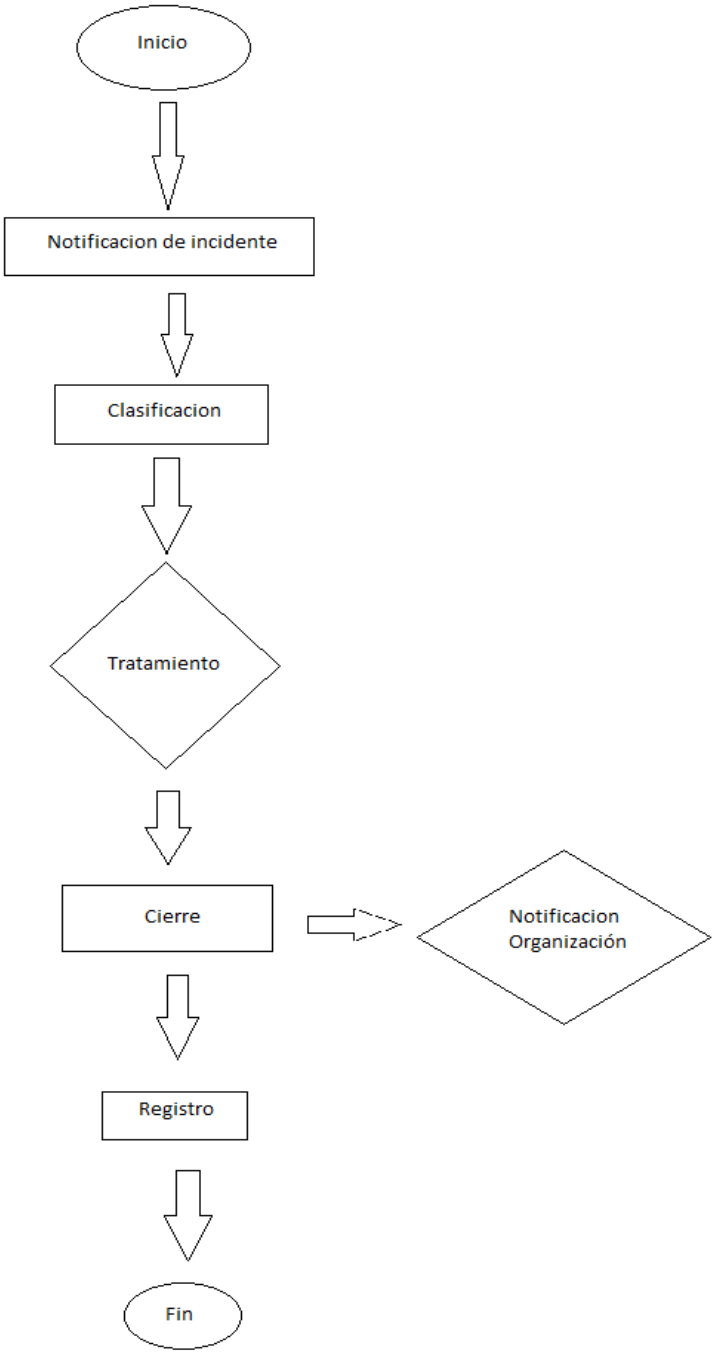
La notificación de cierre se realizará a través del correo electrónico registrado al momento del reporte, en donde se adjuntará el reporte de incidentes diligenciado de acuerdo con la trazabilidad de este (anexo A).

Registro

Notificado el cierre del incidente, el área de Operaciones realizará el registro del reporte generado en la base de datos del CSIRT, en donde se llevará un consecutivo de los incidentes informáticos reportados. En este registro se diligenciarán los campos que lleve el formato del anexo A, con el fin de distinguir a futuro los tipos de incidentes reportados, las fechas y las herramientas utilizadas para dar solución. De esta manera se maneja un registro de incidentes informáticos los cuales funcionaran como precedente o material de apoyo para próximos reportes.

El conjunto de procesos que se cumplen en el procedimiento de la gestión de los incidentes del equipo de respuesta puede identificarse a través de la figura 4, a su vez se observa cual es el flujo de la información en este procedimiento.

Figura 4. Diagrama de Gestión Incidentes



Fuente. Propia del Autor

5.7.10 política de cooperación. A través de esa política la organización define a través de que medios y circunstancias establecerá comunicación y posterior cooperación con entidades externas a la entidad: De la misma manera se establecen los medios de solicitud y entrega de información cuando es requerido.

Objetivo

Establecer los mecanismos de cooperación con otros equipos CSIRT, así como los medios de solicitud de cooperación a “platino Sistemas”.

Alcance

Política aplicable al personal y directivos del CSIRT para la cooperación interinstitucional.

Declaración

El equipo de respuesta a incidentes informáticos CSIRT “platinos Sistemas”, recibirá las solicitudes de cooperación únicamente al correo electrónico del director general, este remitirá al director de Operaciones a través del correo electrónico del CSIRT, el cual evaluará el incidente informático por el cual solicitan cooperación y verificará que hace parte de la clasificación de incidentes interna para brindar la ayuda correspondiente. Si no existe clasificación alguna, se le notificará al director general para que informe de la imposibilidad de brindar la ayuda o cooperación con el caso

Si la cooperación es solicitada para conocer información acerca de los incidentes manejados por le CSIRT Platino Sistemas y estos involucran información sensible de usuarios, debe existir una solicitud formal al director general del CSIRT Platino Sistemas, para evaluar la solicitud y cooperar según lo soliciten.

6 CONCLUSIONES

Aun cuando los mecanismos de seguridad informática en el país no son los más conocidos, Colombia cuenta con instituciones y organizaciones que se encuentran estructuradas para ofrecer mecanismos de seguridad frente a incidentes de carácter informático. Estas han sido constituidas e instauradas a través del gobierno nacional, a cargo de diferentes consejos de seguridad y en donde intervienen varios ministerios o comités administrativos que ofrecen y aportan ideas pertinentes en pro de la seguridad nacional. Gracias al análisis del panorama actual del estado colombiano en materia de ciberseguridad se lograron identificar las principales áreas de amenaza, así como los tipos de ataques con mayor registro, por lo cual se definen los servicios a ofrecer por parte del CSIRT conformado en la empresa PLATINO SISTEMAS, de los cuales destacan el análisis de riesgos, análisis y tratamiento de incidentes y de vulnerabilidades y procesos complementarios como labores de educación y concientización.

A través de diferentes referentes bibliográficos y procesos de recopilación literaria, realizado en el marco del desarrollo del proyecto, se han logrado establecer y determinar los diferentes perfiles profesionales en las áreas directivas, operacionales y de apoyo profesional del CSIRT para la empresa PLATINO SISTEMAS. En este proceso se lograron identificar y definir claramente el enfoque académico profesional, la experiencia requerida para cada uno de los cargos y las dependencias a las que estos pertenecen. En medio de este proceso se identificaron las áreas de dirección general, dirección operacional y de dirección de Tecnologías de la información, lo cual permitió crear un diagrama jerárquico que permite identificar de manera clara la estructura organizacional del CSIRT, donde se crean las dependencias mencionadas y los cargos que pertenecen a estas.

PLATINO SISTEMAS dentro de su catálogo de servicios, ofrece a sus usuarios apoyo en las áreas de seguridad informática en las cuales así lo requieran. Apoyado en la norma ISO/IEC 27001, más exactamente en el Anexo A y el listado de controles allí propuestos para los SGSI, se ha logrado precisar las políticas y procedimientos operacionales bajo los cuales se regirán todas las actividades del equipo de respuesta. De esta manera para cada incidente informático reportado existen los procedimientos adecuados para su atención y solución, los mecanismos y formatos de recepción de este, así como las medidas para mantener la privacidad y tratamiento de los datos, asegurando así, la confidencialidad de la información tratada.

7. RECOMENDACIONES

Las políticas y procedimientos operacionales mencionados en este documento, son los mínimos obligatorios para que cualquier CSIRT entre en funcionamiento y asegure a sus usuarios los mínimos procesos para garantizar que las labores realizadas dentro del equipo cumplen con procesos estandarizados y de calidad; pero queda a disposición del director general del equipo de respuesta, formularse otras políticas que se crean adecuadas en medio del desarrollo cotidiano del CSIRT y que estén ajustadas a la normativa nacional o internacional.

La cantidad de personal a nivel técnico es sugerida para un CSIRT de tamaño mediano. El director general del equipo de respuesta deberá evaluar la necesidad de incluir más personal de carácter técnico o de apoyo profesional de acuerdo con la cantidad de reportes de incidentes que se reciban.

El catálogo de servicios para el CSIRT Platino Sistemas está enfocado a brindar la ayuda necesaria a incidentes informáticos sensibles de ser solucionados a través de canales virtuales o a distancia, a través de conexión remota o brindando el soporte requerido a través de encuentros síncronos y asíncronos. Si se contemplan las asistencias *in situ* o en el lugar del incidente, se deberán adecuar las medidas y procedimientos necesarios para estos, así como contar con las políticas necesarias para asegurar la calidad del servicio.

Anexo A. Formato Reporte incidentes

"Platinos Sistemas" CSIRT	Reporte de incidentes	Version:01-17-10-2020

Reporte de Incidente

Información General

Consecutivo_____

Nombre de quien reporta incidente. _____

Correo electrónico de contacto. _____

Cargo en la organización. _____

Fecha de reporte _____

Oficina o dependencia. _____

Hora de reporte. _____

Contacto telefónico _____

Personal que atiene el reporte _____

Descripción del incidente.

_____

_____

Clasificación Incidente

Área asignada al tratamiento _____
Responsable _____
Fecha de recepción _____
Hora de recepción _____

Tratamiento

In situ (Opcional)

Lugar de desplazamiento_____
Fecha de desplazamiento_____
Área encargada: (marque con una "X")
Dirección TI ( ) dirección Operaciones ( ).
Profesional responsable _____
Herramientas utilizadas _____

“Platinos Sistemas” CSIRT	Reporte de incidentes	Version:01-17-10-2020

Canal Virtual

Àrea encargada.
(marque con una “X”)
Dirección TI ( ) dirección Operaciones ( ).
Profesional responsable _____
Herramientas utilizadas _____

Cierre

Fecha cierre_____
Hora cierre _____
Correo de Notificación _____

BIBLIOGRAFIA

Agencia Europea de Seguridad de las Redes y de la Información, ENISA (2006). Cómo crear un CSIRT paso a paso. Recuperado de: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

ASOBANCARIA. (2018). Implementación y puesta en marcha CSIRT para el sector financiero. Recuperado de https://www.asobancaria.com/wp-content/uploads/CSIRT-Financiero-Asobancariajulio-2018.pdf

BALDERRAMA, J. (2017). Como crear un CSIRT Fundamentos. [Video Youtube] Recuperado de https://www.youtube.com/watch?v=2huboveQFLs

Centro Criptológico Nacional CCN de España. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [en línea]. [Consulta abril 13 de 2020]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-

Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

Council Of Europe. Serie de tratados europeos. Convenio Sobre la Ciberdelincuencia. [en línea]. [consulta: abril 17 de 2020] Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

DE LA TORRE MOSCOSO, Hugo Marcelo, Parra Rosero, Mario Andrés (2018). Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE.

Carrera de Ingeniería en Sistemas e Informática. Universidad de las Fuerzas Armadas ESPE. Matriz Sangolquí. Recuperado de: http://repositorio.espe.edu.ec/handle/21000/15071

Departamento de derecho internacional OEA. Resolución asamblea general. AG/RES. 2040 (XXXIV-O/04). [en línea]. [Consulta: abril 17 de 2020]. Disponible en: http://www.oas.org/juridico/spanish/ag04/agres_2040.htm

Dinero. Colombia incremento en un 70% sus conexiones a internet en ocho años. [en línea]. [Consulta: 23 de abril de 2020]. Disponible en: https://www.dinero.com/pais/articulo/balance-conexiones-a-internet-en-colombia-2010-2008/260104

E CAROZO, C MARTINEZ, L VIDAL, G BETARTE, A BLANCO, E COTA, J PÉREZ, (2006). CERTuy: Hacia un CSIRT Nacional. Recuperado de: https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom-013.pdf

El tiempo. (2019). Las tácticas que amenazan su seguridad informática. Recuperado de: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-ataques-de-cibercriminales-en-colombia-371096

El Tiempo. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. [en línea] [Consulta: abril 24 de 2020]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

FIRST.org. (2019). Forum of Incident Response and Security Teams, por sus siglas en inglés. Recuperado de https://www.first.org/

G, f i r s t . o r. (2016). Foro sobre los equipos de seguridad e intervención 2 en caso de incidente (FIRST.Org). Recuperado de

https://www.first.org/education/FIRST_SIRT_Services_Framework_Version1.0-es.pdf

GUERRERO, J. Incidentes informáticos en Colombia en los últimos 10 años. [Internet]. 2018. [citado: 2020, abril] Disponible en: https://repository.unad.edu.co/handle/10596/31941

HUERTAS, L. (2016). Estructura interna de un CSIRT. [Video Youtube] Recuperado de https://www.youtube.com/watch?v=RaBp3qsxQYY

INCIBE. Control de Acceso, Política de seguridad para Pyme. [en línea]. [Consulta: 6 de octubre de 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf

INCIBE. guía sobre borrado seguro de la información. [en línea]. [Consulta: 3 octubre de 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

KITCHENHAM, B., (2004) Procedures for Performing Systematic Reviews, TR/SE-0401, Keele University.

Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, Dirección Nacional de Inteligencia, D. N. de P. (2016). POLITICA NACIONAL DE SEGURIDAD DIGITAL. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

OEA. (2016). Buenas Prácticas para establecer un CSIRT nacional. Recuperado de https://www.sites.oas.org/cyber/Documents/2016 - Buenas Prácticas CSIRT.pdf

Oracle. ¿Qué es el Spoofing? [en línea]. [Consulta: abril 27 de 2020]. Disponible en: https://www.oracle.com/es/database/security/que-es-el-spoofing.html

Panda Security. Criptojacking. [en linea]. [Consulta: abril 27 de 2020]. Disponible en: https://www.pandasecurity.com/es/security-info/cryptojacking/

PLANEACIÓN, DEPARTAMENTO NACIONAL DE, Ministerio de Tecnologías de la Información y las Comunicaciones, S. de I. y C. (2018). POLÍTICA NACIONAL DE EXPLOTACIÓN DE DATOS (BIG DATA). Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3920.pdf

Ron Egas, M, Vasquez Cañas, R. Lanfranco, E. Macia, N. & Diaz, J. (2017) Practical Guide To Implement An Academic Computing Security Incident Response Team (Academic CSIRT)

Secretaria senado, ley 1273 2009, [en línea]. [Consulta abril 10 de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

WEST-BROWN, M., STIKVOORT, D., KOSSAKOWSKI, K., KILLCRECE, G., RUEFLE, R. & ZAJICEK. M (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). Pittsburgh. Carnegie Mellon

VAN DER HEIDE, M. (2017). Establishing a CSIRT. Thailand: Thailand Computer Emergency Response Team.

Welivesecurity. Martes de retrospectiva: el gusano Morris. [en línea]. [Consulta: octubre 5 de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris/